Reliability assessment of redundant safety systems with degradation

Rogova, Elena

DOI
10.4233/uuid:17606183-f86f-45c4-8333-417dce87392f

Publication date
2017

Document Version
Final published version

Citation (APA)
Rogova, E. (2017). *Reliability assessment of redundant safety systems with degradation*. [Dissertation (TU Delft), Delft University of Technology]. https://doi.org/10.4233/uuid:17606183-f86f-45c4-8333-417dce87392f

Reliability Assessment of Redundant Safety Systems with Degradation

Elena Sergeevna Rogova

Reliability Assessment of Redundant Safety Systems with Degradation

Proefschrift

ter verkrijging van de graad van doctor
aan de Technische Universiteit Delft
op gezag van de Rector Magnificus prof. ir. K.C.A.M. Luyben,
voorzitter van het College voor Promoties,
in het openbaar te verdedigen op 7 Juli 2017 om 15:00 uur

door

Elena Sergeevna ROGOVA

Engineer-Physicist,
National Research Nuclear University (MEPhI), Moskou, Rusland
Geboren te Penza, USSR

This dissertation has been approved by the
promotor: Prof. dr. ir. G. Lodewijks

Composition of the doctoral committee:

Rector Magnificus	Delft University of Technology, chairperson
Prof. dr. ir. G. Lodewijks	Delft University of Technology, promotor

Independent members:

Prof.dr. P.H.A.J.M. van Gelder	Delft University of Technology
Prof.dr. G. Jongbloed	Delft University of Technology
Prof.dr. A. Grall	University of Technology of Troyes
Prof.dr. V.I. Didenko	National Research University (Moscow Power Engineering Institute)
Dr. N. Brinzei	University of Lorraine

Other member:

Prof.dr. M.A. Lundteigen	Norwegian University of Science and Technology

This research was funded by De Stichting Nederlands Instituut voor Lifttechniek, Amsterdam, Grant P90863.

Published and distributed by: E.S. Rogova
E-mail: e.rogova88@gmail.com
Keywords: reliability, safety systems, failure rate function, degradation, redundancy

ISBN 978-94-6233-662-9
An electronic version of this thesis is available at `http://repository.tudelft.nl/`.

Printed in the Netherlands

To my parents and my brother

Preface

First of all, I would like to thank my daily supervisor and promotor Prof.dr.ir. Gabriel Lodewijks for inviting me to work as a PhD-researcher in the Section of Transport Engineering and Logistics at the Department of Maritime and Transport Technology. He always provided me with valuable comments on my work and gave me suggestions on how to improve my research despite his very busy schedule. Thanks to Prof. Lodewijks I managed to become an independent researcher.

I would like to express my gratitude to Prof. Mary Ann Lundteigen for giving me the possibility to take her course “Reliability of safety-critical systems” at NTNU, and for her invaluable contribution as a co-author of conference and journal papers. Many thanks to Prof. O.A. Golovanov for mathematical consultation, Prof. A.P. Elokhin, Dr. Antonio Vergara Fernandez and Dr. Eduardo Calixto.

Special thanks to Dick Mensch for his support during my staying in Delft, his help with Dutch language and proof checking of my thesis. Big thanks to Josephina Spoek-Schouten, Dineke Heersma and all secretaries who were always willing to help. Thanks to Dr. Yusong Pang, Kanu Priya Jain, Guangming Chen, Shijie Li, Lindert Biert, my officemates and all my colleagues. Of course I would like to say many thanks to my sponsor De Stichting Nederlands Instituut voor Lifttechniek for their financial support and valuable comments. A big thanks goes to CERN which provided with practical data for this research, especially machine protection group and cryogenics group.

I would like to say thanks to Natalia Vturina and Mikhail Belonosov who always invited me to their welcoming house. Many thanks to Nikita Lenchenkov, Nick Gayko, Mikhail Davydenko, Alan Zangiev, Gleb Polevoy, Alieh Kazemi and her husband Matheus, Victoria Hancock, Dmitrii Boitcov, Anastasia Holovchenko, Dima Afanasiev, Maria Fravventura and Gabriele Bulgarini. I also thank all my friends in the Netherlands, Russia and around the world.

I would like to thank Pasquale Scarlino for his support and exploring with me different sides of our wonderful life. Many-many thanks to my dear brother Andrei for his help, support and our Skype-discussions on numerous topics. Finally I would like to thank very specially my dear parents, Svetlana and Sergei. You gave me everything, and even more. Your endless love and support are always with me.

Elena Rogova
Delft, May 2017

Contents

Chapter 1

Introduction

Escalators, elevators and moving walks are used as equipment to transport people primarily in public infrastructure such as supermarkets, airports, railway stations, buildings and the underground. These machines can be of different types. For example moving walks can be horizontal or inclined. Elevators can be classified according to their hoist mechanism as hydraulic, traction, and pneumatic elevators (Strakosch, 1998). The main purpose of all this equipment is to move people, and to do this safely.

Safety is a big issue for people transportation equipment. The history of elevator safety devices was started from the invention of the first mechanical safety device to prevent the free fall of the lifting platform. This was done by Elisha Graves Otis in 1853 (Strakosch, 1998). Safety systems of elevators were significantly improved since that time by adding additional safety mechanical and electronic devices.

Each machine has several safety-related systems. A safety-related system in escalators and moving walks is defined by the standard ISO 22201-2 as one or more safety devices performing one or more safety functions that may be based on programmable electronic systems (PES), electrical, electronic and/or mechanical elements of the lift (ISO 22201-2, 2013). A general definition of all safety-related systems is given in the standard IEC 61508 (IEC 61508-4, 2010).

1.1 Safety systems of people transportation equipment

Modern safety devices become more and more “clever” by adding electronics. Safety devices that recently were only of mechanical type, now are supplemented or replaced with devices of electronic type. All these changes have as the main purpose: to make people transportation equipment as safe as possible. Adding electronic infrared sensors to the mechanical door operators or laser rangefinders to safety relays for car levelling creates redundancy for existing before only mechanical or electro-mechanical safety devices. Such safety systems become more complicated with a more difficult “mixed” architecture. Mixed safety systems, which contain both mechanical and electronic components, are called heterogeneous safety systems in this dissertation. Heterogeneous redundancy is defined as redundancy with mixing of different types of components (Sharma et al., 2011). Therefore this redundancy architecture has different channels: some channels contain electronic components, others - mechanical.

Examples of safety devices and heterogeneous redundant safety systems of escalators and elevators are presented in the next sections.

1.1.1 Safety systems of escalators

In accordance to Mitsubishi Electric (Mitsubishi Electric, 2016), there are sixteen basic safety devices of escalators. Location of these devices is shown in Figure 1.1. The target of these devices is to prevent accidents and to protect passengers. Safety devices of moving walks are not discussed here because the principle of work of escalators and moving walks is very similar, as well as the safety devices.

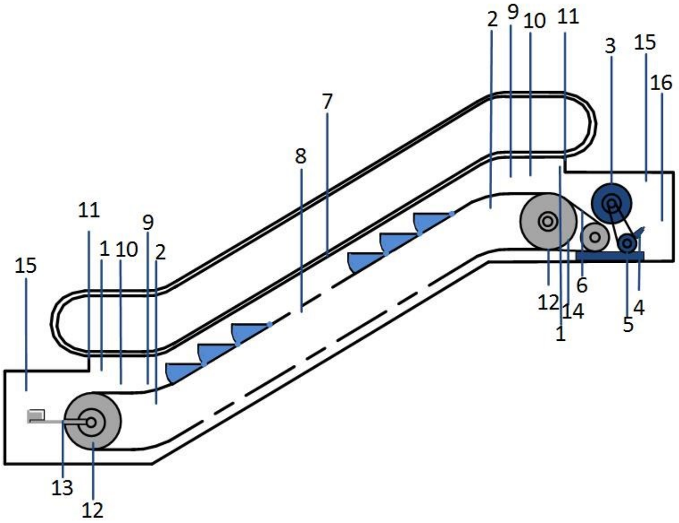


Figure 1.1: Location of escalator safety devices.

1) The first device is *Emergency Stop Button.* In case of emergency (for instance, falling of people on a moving surface etc.) every passenger can push the button which is located in a well-observable place. This button will immediately activate the braking system of the escalator (Mitsubishi Electric, 2016).
2) The *Step Motion Safety Device* activates the braking system which stops the escalator in case of dislocation of steps due to an object between steps, or between the skirt guard and the step, or in case of abnormality in the step motion (Mitsubishi Electric, 2016).
3) The escalator has to be stopped by the *Overload Detection Device* in case of overload detected by abnormal current or temperature of the drive motor (Mitsubishi Electric, 2016).
4) The *Speed Governor* stops the escalator if the speed significantly decreases or increases to 120% of the rated speed (Mitsubishi Electric, 2016).
5) The *Electromagnetic Brake* (another option is *Hydraulic brake*) - a safety device that stops the escalator in the case of power failure, or if any safety device or the Emergency Stop Button has been activated (Mitsubishi Electric, 2016).
6) The *Drive Chain Safety Device* stops the escalator by applying the safety brake on the drive shaft if the Drive Chain breaks or stretches beyond an allowable value (Mitsubishi Electric, 2016).
7) The *Handrail Speed Safety Device (HSS)* has to stop the escalator if the *Moving Handrails* fail to synchronize with the Steps due to slippage, loosening or breakage of the *Moving Handrails*. There is a handrail speed sensor that measures the variation in speed between the steps and handrail. If speed variation becomes too large, the controller has to turn off power and to activate the brake to stop the escalator (Kone, 2007).
8) If the horizontal level of a Step has dropped, *Step Level Device* has to stop the escalator (Mitsubishi Electric, 2016).
9) A shoe or a long coat or other items may be trapped between the step and a skirt guard. In this case *Skirt Guard Safety Device* has to stop the escalator (Mitsubishi Electric, 2016).

10)-16) *Auxiliary brakes (14)* are not always required to be installed in escalators (as stated in EN 115-1, 2010). It is a mechanical device which stops the escalator if the speed exceeds the rated speed, or other abnormalities. The *Comb-Step Safety Switch (10), Handrail Guard Safety Device (11), Missing*

Step Device (12), Step Chain Safety Device (13), Door Open Switch (15) and Three elements (16) are other safety devices which are also installed in the escalator (Mitsubishi Electric, 2016).

All these safety devices detect a specific problem and stop the escalator. Therefore among these sixteen safety devices one should be considered with a special attention: the braking system itself. The majority of possible accidents can be prevented by the timely stop of the escalator (due to falling of people or malfunction of other escalator devices). Therefore a braking system acts as a final actuator in all malfunctions and accidents.

Failure of a braking system can cause serious consequences like accidents with people injuries and even deaths. The Washington Post describes an escalator accident, when 6 metro passengers were injured. “Overspeed fault”, which shut down the escalator’ motors, automatically engaged the brakes. Officials said that all three brakes engaged, but failed to slow down the escalator. The first brake was covered in oil, the second “showed wear” and the third was in “good condition” (Scott Tyson A., 2010). The report “Assessment of Elevator and Escalator Maintenance & Repair Program Final Elevator Audit Submission”, among others, identified the following problems of braking system of escalators and moving walks detected during inspections: incorrectly adjusted and/or damaged brake systems; brake pads are worn and need replacement; escalator brakes have questionable stopping performance under no load. Some brakes of escalators were scheduled for replacement after inspection (VTX, 2010).

1.1.2 Safety systems of elevators

Figure 1.2 shows the various protective and safety devices of a traction elevator. These safety devices are located in the machine room, in the hoistway, on the car, and in the pit.

Overspeed of the car is monitored by the G*overnor*, which cuts off power if a certain speed is exceeded and causes the M*echanical safety devices* located on the car frame to actuate and lock the car to the G*uide rails* if the speed continues to increase. The definition of the overspeed governor is given by the standard EN 81-1 for electric lifts. It is “a device which, when the lift attains a predetermined speed, causes the lift to stop, and if necessary causes the safety gear to be applied" (EN 81-1, 1998). From the mechanical design aspect, overspeed governors may be of centrifugal or pendulum type (Janovsky, 1993).

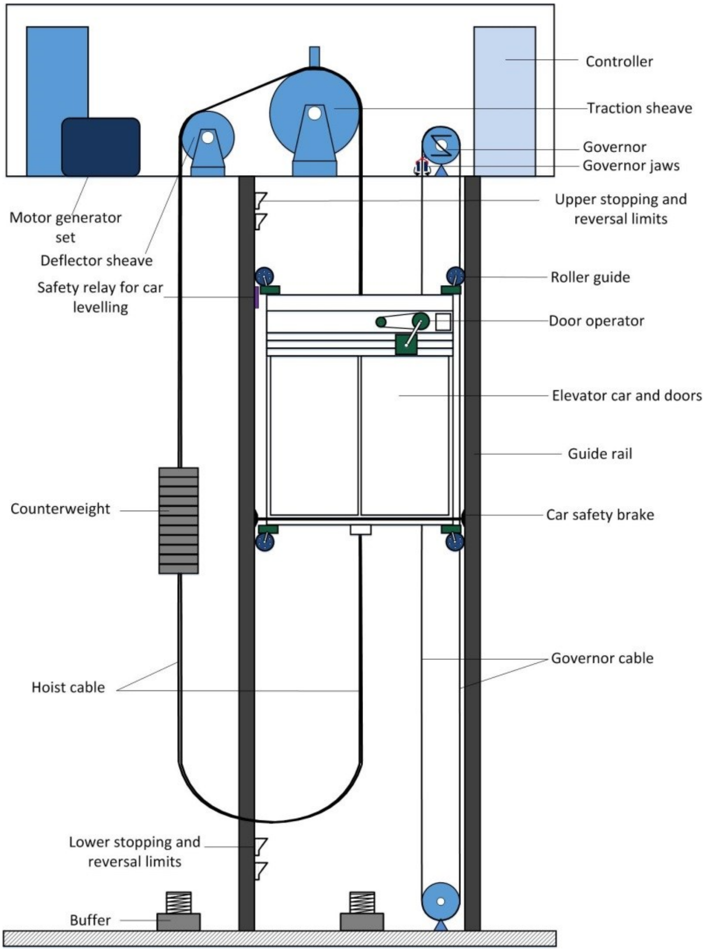


Figure 1.2: Safety devices of elevators.

The principle of work of the centrifugal overspeed governor can be described as follows. If the car speed exceeds the allowable limit, the flyweights move outside due to the centrifugal force and actuate an overspeed switch. This switch turns off the power of the elevator. If the speed of the car continues to grow, the moving of the flyweights actuates a special latching device that in normal condition holds a swinging jaw of the governor (Janovsky, 1993).

“When the swinging jaw is released it clamps the *Governor rope* against the fixed jaw. This jaw is spring-loaded and pre-set by an adjusting bolt to give the tension required in the governor rope to operate the S*afety gear* as the governor rope slides through the jaws during the safety gear operation” (Janovsky, 1993).

Nowadays there are also electronic overspeed governors. The principle of work is based on signals obtained from the incremental encoder (magnetic or optical). The encoder sends a certain number of pulses per revolution of the encoder disk. If the time between neighboring pulses decreases, the overspeed is detected, and the brakes are actuated. Such governors are much smaller, and quieter. However, often electronic governors are used in a redundancy architecture together with a mechanical overspeed governor. This is an example of a heterogenous safety system.

Besides the overspeed, there is a problem with failure to stop at the limits of travel. The *Lower Stopping switches* operate to cut off power and apply the brake to the machine. Continued travel of the car into the pit is stopped by the *Buffer*, as is continued travel of the car into the overhead wherein the *Counterweight buffer* is used (Stracosch, 1998).

The Door operator plays an important role. According to statistics, more than 80% of the elevator accidents and 70% of the elevator faults are caused by the door system among all kinds of elevator accidents (Lu et al., 2012). The hoistway doors have to be protected from opening during the normal operation unless the elevator car is stopped in the landing zone. The locking of doors is performed by the *Hoistway Door Interlock* (Janovsky, 1993). Door operator also has another function: to not hit/trap passengers between doors. *Door operator* is connected to the *UCMP (Unintended Car Movement Protection) device*.

The most popular modern solution for sensors which are used for elevator doors is the *Light curtains*. They are based on infrared technology. Old models of elevators do not have such sensors. Such doors are equipped by M*echanical safety edges*: the door will open again if they detect physical contact. Therefore door operators of new elevators have redundant heterogeneous system of item detection between elevator doors: the first one is mechanical and the second one is electronic (infrared sensor).

Another example of mixed (heterogeneous) redundancy by using mechanical and electronic components can be found in a system of car levelling. The elevator car has to be stopped at the landing zone. The responsible component is *Safety relays for car levelling*. Relays are electro-mechanical components, and they can be affected by wear. The possible solution is application of redundancy by using an alternative way of level measuring: laser rangefinder. In this case laser rangefinder is installed in a shaft of the elevator, and gives a very precise levelling signal to the main controller.

1.2 Reliability quantification

Safety systems of people transportation equipment perform safety functions to save life and health of passengers. However people still get injured and even die on escalators, elevators, and moving walks. Unfortunately such accidents cannot be eliminated completely. However the amount of these accidents and severity of consequences can be significantly reduced by enhancement of reliability of safety critical systems. Such improvements can be done by introducing a diagnostic system, performing maintenance, by applying redundancy for critical components, by replacement of them, or by combination of these approaches. Replacement and redundancy of old mechanical components have the purpose to increase the safety of the machines by enhancement of reliability. Therefore it is required to quantify reliability before and after applying redundancy or replacement of an old mechanical component by a new one (electronic/electrical/mechanical) because reliability assessment is the only way to prove that the system became more reliable which means safer.

Channels of heterogeneous redundant architecture have different physical principles due to mechanical and electronic/electrical components and different failures: random failures without degradation for electronic channels and degradation (wear) –for mechanical channels (Figure 1.3). Therefore failure rates, the rates at which failures occur as a function of time, (Rausand and Hoyland, 2004), of mechanical and electronic components are different. For electronic components they are mainly constant, for mechanical – non-constant. Mechanical components with degradation often require a calculation of the failure rate function. Heterogeneous redundant architecture that contain channels with constant and non-constant failure rates can be found not only in safety systems of people transportation equipment, but also in other safety-related applications such as oil and gas, nuclear, chemical, and aerospace.

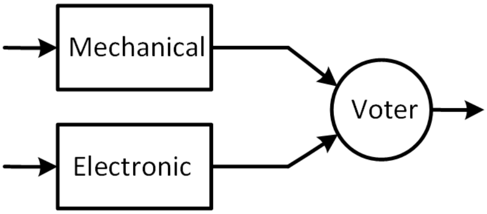


Figure 1.3: Redundancy architecture.

Reliability assessment of heterogeneous safety systems is considered in the literature. However, existing methods are mainly focused on existing heuristic algorithms and some difficulties related to optimization problems and do not aim at a practical calculation of system reliability in the concept of functional safety. There is a lack of practical methods of reliability assessment of heterogeneous redundant architectures with different channels and combination of constant and non-constant failure rates (Rogova and Lodewijks, 2016).

The conducted literature review showed that the problem of reliability assessment of redundant safety systems and systems with non-constant failure rates modelled by Weibull distribution, is well covered by literature as will be shown in Chapter 2. This research is focused on the lacking part in the current state of the art: analytical formulas of $\mathrm{PFD}_{\mathrm{avg}}$ (average probability of failure on demand) and PFH (average frequency of dangerous failure) calculation of M-out-of-N redundant safety systems with non-constant failure rates; development of analytical method of reliability assessment of heterogeneous M-out-of-N repairable systems with degradation, different channels and possibility to model different states of a system.

Analytical formulas of $\mathrm{PFD}_{\mathrm{avg}}$ calculation for systems with non-constant failure rates have been considered by Jigar (Jigar, 2013). This work has been taken as a basis and improved with adding CCF (common cause failures) contribution and involving a failure rate function to the formulas. The literature review of analytical formulas of PFH calculation of M-out-of-N systems with degradation did not reveal their existence.

Literature review of analytical methods of reliability assessment of M-out-of-N repairable systems with degradation and different channels directed us to semi-Markov methods. These methods have been considered by Limnios and Oprisan (2001), Kumar et al. (2013), Grabski (2014) and other researchers. Perturbed Markov methods and continuous semi-Markov methods are very limited in application, and often are not applicable for the analysis of the described system. The main disadvantage of the steady-state semi-Markov method is its inapplicability for transient analysis. Taking into account these limitations, the new window-based Markov method has been developed in this thesis. This method is applicable for transient analysis, has a high accuracy and easy for practical implementation.

Development of described analytical formulas and analytical method is required to obtain PFD_{avg} and/or PFH values for making a decision about sufficient safety level after applying redundancy. Obtained values participate in making a choice between replacement and redundancy as a way to enhance reliability, together with discussion of changing architecture and economic question.

1.3 Research questions

The main research question of this dissertation:

How to quantify the reliability of redundant safety systems with degradation?

Modernization of escalators, elevators and moving walks involves more and more the installation of electronic components by replacing the old mechanical components and applying redundancy. The reason for this trend is safety improvement since safety is very important in people transportation equipment. This change of components has to be justified by a higher level of reliability. The reliability has to be calculated and compared in two cases: before and after applying redundancy. This can be done by simulation or by a theoretical approach which includes development of analytical formulas and methods of reliability assessment. In this dissertation a theoretical approach will be used for the reliability assessment of heterogeneous safety systems together with a simulation part and data obtained from exploitation of mechanical equipment.

The sub-questions of this dissertation are following:

1. **Which methods and safety standards are available for reliability assessment of redundant safety systems?**

   In accordance to the functional safety approach a safety system performs a safety function. Each safety function has Safety Integrity Level (SIL) requirements. The safety integrity level of a safety system has to correspond to the SIL-requirements of a safety function. Each SIL has a range of PFD_{avg}/PFH values. These values can be estimated by using different reliability assessment methods. Review of safety standards for escalators, elevators and moving walks identifies the existence of analytical formulas which can be used for reliability calculation. However analytical formulas presented in the standards do not work for systems which contain components with non-constant failure rates. The survey of reliability assessment methods shows that they are not always applicable for heterogeneous safety systems.

2. **How can the functional safety concept be used as a criterion for applying redundancy of a braking system of moving walks?**

   The braking system of moving walks is a very important safety critical system. In case of any kind of an accident the machine has to be stopped. Therefore reliability of this system has to meet the requirements. In accordance to the functional safety concept it is necessary to know whether the braking system corresponds to SIL requirements or not. Based on this, the decision about applying redundancy and/or development of a diagnostic system can be made. If the PFD_{avg}/PFH values of a braking system correspond to SIL-requirements, such safety system is considered as reliable. If calculated PFD_{avg}/PFH values do not correspond to SIL requirements, a braking system requires reliability enhancement, and applying redundancy together with diagnostic system can be recommended.

3. **Which analytical formulas can be developed for PFD_{avg}/PFH calculation of redundant safety systems with non-constant failure rates?**

   Analytical formulas are always welcomed by practitioners due to their convenience in application. Unfortunately the analytical formulas of PFD_{avg}/PFH calculation presented in the safety standards (IEC 61508-6, 2010) can be applied only to redundant safety systems with constant failure rates. Therefore it is necessary to develop analytical formulas which can deal with reliability assessment of redundant safety systems with non-constant failure rates.

4. **How does the developed window-based Markov method overcome the limitations of the developed analytical formulas for reliability assessment?**

   The developed analytical formulas of PFD_{avg}/PFH calculation are able to calculate reliability of redundant safety systems with non-constant failure rates. However these formulas work only for a redundancy architecture with identical channels with non-constant failure rates. If a redundancy architecture is heterogeneous, it contains non-identical channels with mechanical components (with non-constant failure rates) and channels with electronic components (with constant failure rates). Therefore such an architecture requires development of a new method.

5. **How can the failure rate function be obtained practically?**

   The Weibull distribution is used in this dissertation for mathematical modelling of mechanical degradation. The parameters of this distribution are used for calculation of non-constant failure rate (failure rate function). Theoretically, Weibull parameters can be taken from reliability handbooks and Weibull databases. However the accuracy of a failure rate function obtained in such a way is not high because in this case the parameters do not account operating conditions and a manufacturer. Weibull parameters have to be obtained based on raw degradation data of components if such data is available. Therefore it is desirable to obtain the failure rate function practically based on raw monitored data. However practical obtaining of Weibull parameters has some issues such as an exact definition of failure mode, quality of data. Therefore it is important to present practically obtained failure rate functions.

6. **What is the criterion of choice of the architecture in safety systems with degradation?**

   A functional safety approach together with the developed analytical formulas and methods of reliability assessment are used for reliability quantification and understanding of correspondence to SIL-requirements. This helps in making a decision about reliability enhancement. However the final decision about the choice of architecture, besides of reliability assessment, includes the question of changing architecture and the economic question. These aspects have to be accounted all together to make a decision about an appropriate architecture of a safety system.

1.4 Research methodology

The main approach which is used in this dissertation is a functional safety concept. This concept allows to work with SIL requirements as a criterion of sufficient reliability. Functional safety also proposes a procedure how to determine SIL-requirements if such requirements are not defined by the standard.

The dissertation uses mainly a theoretical approach in the development of analytical formulas and methods of reliability assessment. The correctness of the developed window-based Markov method is validated by the results obtained by a Monte-Carlo simulation.

This thesis also contains an experimental part where the failure rate function is obtained based on raw monitored data of mechanical components.

1.5 Outline of this Dissertation

The outline of this dissertation is presented in Figure 1.4.

Chapter 2 describes available methods of risk and reliability assessment of heterogeneous safety systems of escalators, elevators and moving walks, and considers recommendations of the standards. This chapter determines existing problems and bottle necks of the methods.

The functional safety approach described in *Chapter 3* is used for the determination the necessity of redundancy of degrading components/subsystems as a part of safety systems. It is considered on the basis of a braking system of moving walks.

Chapter 4 compares several methods of reliability assessment of heterogeneous redundant systems: new analytical formulas of PFD_{avg} (Average Probability of Failure on Demand) and PFH (Average Frequency of Dangerous Failures) calculation and steady-state semi-Markov methods.

Chapter 5 presents a new window-based Markov method for a reliability assessment of heterogeneous safety systems and systems with heterogeneous redundancy architecture and provides the results of simulation.

Chapter 6 is the practical part of the dissertation. Due to a lack of statistical data of degradation of mechanical components in escalators, elevators and moving walks, the failure rate function is obtained by using available data from cryogenic control valves. This chapter demonstrates “cleaning” and filtering of raw degradation data, presents the algorithm for obtaining a failure rate function of real degrading mechanical components based on the example of cryogenic slide valves.

In *Chapter 7,* obtained practical failure rate functions are used in the developed decision scheme for the choice of architecture that include calculation of availability, reliability and replacement costs.

Chapter 8 concludes and provides proposals for future research. Here the reader can find recommendations for further development of proposed analytical methods of reliability assessment. The possible directions for application of the developed methods in practice is also discussed in this Chapter.

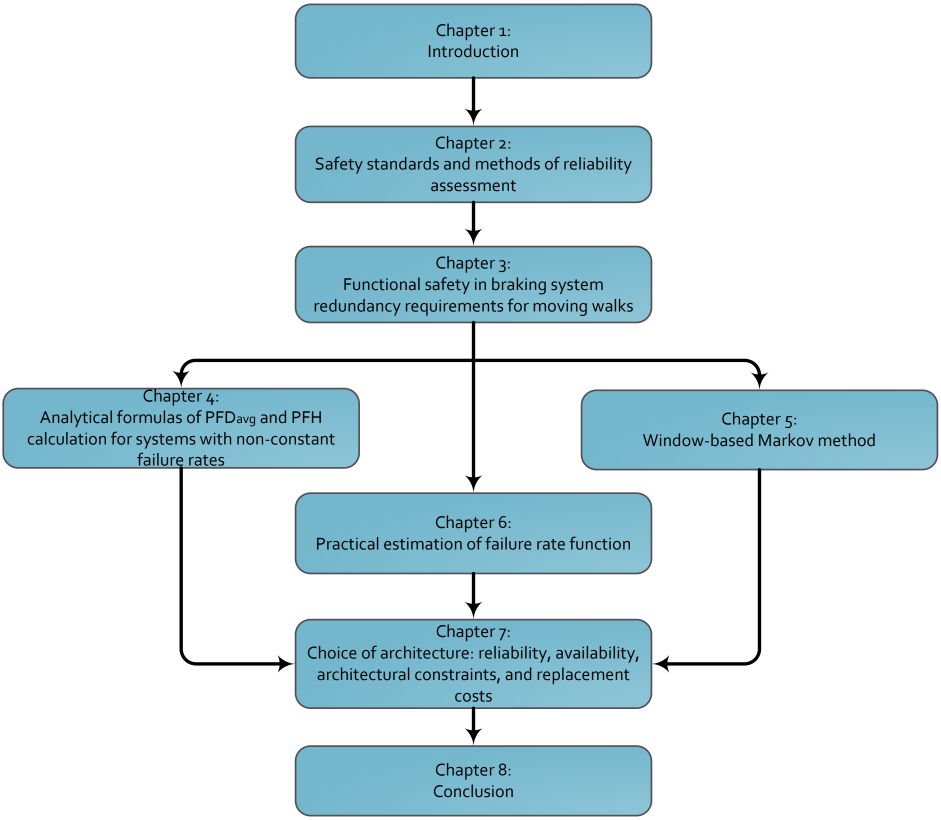

Chapter 1:
Introduction
Chapter 2:
Safety standards and methods of reliability assessment
Chapter 3:
Functional safety in braking system redundancy requirements for moving walks
Chapter 4:
Analytical formulas of PFDavg and PFH calculation for systems with non-constant failure rates
Chapter 5:
Window-based Markov method
Chapter 6:
Practical estimation of failure rate function
Chapter 7:
Choice of architecture: reliability, availability, architectural constraints, and replacement costs
Chapter 8:
Conclusion

Figure 1.4: Thesis outline.

References

Kone (2007) *Escalator Safety and Performance Upgrades.* Available at https://toolbox.kone.com/media/en_US/pdfs/KONE%20Escalator%20Safety%20and%20Performance%20Upgrades%20SF2857%20Rev0107.pdf?rdrsrc=/media/en_US/pdfs/KONE%20Escalator%20Safety%20and%20Performance%20Upgrades%20SF2857%20Rev0107.pdf&rdrtrg=https://toolbox.kone.com/media/en_US/pdfs/KONE%20Escalator%20Safety%20and%20Performance%20Upgrades%20SF2857%20Rev0107.pdf (Accessed 2 November 2016).

European Committee for Standardization (CEN) (1998) *EN 81-1. European standard Safety rules for the construction and installation of lifts -Part 1: Electric lifts.*

European Committee for Standardization (CEN) (2010) *EN 115-1+A1. Safety of escalators and moving walks – Part1: Construction and installation.*International Electrotechnical Commission (IEC) (2010) *IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations.*

International Organization for Standardization (ISO) (2013) *ISO 22201-2. Lifts (elevators), escalators and moving walks – Programmable electronic systems in safety related applications – Part 2: Escalators and moving walks (PESSRAE).*

Janovsky, L. (1993) *Elevator mechanical Design.* 2nd edn. Bodmin: Ellis Horwood Ltd., pp. 211-212.

Lu, Z.-Y., Zhao, B., Liu, T., Song, Y.-P. and Zhang, Y.-M. (2012) 'Video detection system design of meshing depth of elevator's door lock', *Advanced Materials Research*, ***580***, pp. 231-235.

Mitsubishi Electric (2016) *Locations of Key Safety Devices.* Available at: http://www.mitsubishielectric.com/elevator/overview/e_m_walks/e_s_equipment03.html (Accessed 4 October 2016).

Rausand, M. and Høyland, A. (2004) *System Reliability Theory. Models, Statistical Methods, and Applications*. 2nd edn. Hoboken, NJ: John Wiley & Sons.

Rogova, E. and Lodewijks, G. (2016) Methods of reliability assessment of heterogeneous redundant systems. Proc. *8th IFAC Conference on Manufacturing Modelling, Management and Control MIM 2016*, Troyes, France, IFAC-PapersOnLine, 49(12), pp.139–144.

Scott Tyson, A. (2010) 'Metro escalator brake, maintenance problems widespread', *The Washington Post,* 14 Nov.

Sharma, V.K., Agarwal, M. and Sen, K. (2011) 'Reliability evaluation and optimal design in heterogeneous multi-state series-parallel systems', *Information Sciences* ***181(2)***, pp. 362–378.

Strakosch, G.R. (1998) *The Vertical Transportation Handbook*. 3rd edn. USA: John Wiley & Sons, Inc.

VTX – Vertical transportation Excellence (2010). *The audit report "Assessment of Elevator and Escalator Maintenance & Repair Program Final Elevator Audit Submission"*. Available at: http://media.washingtonpost.com/wp-srv/metro/documents/metro_escl_report_pages151-225.pdf (Accessed 4 October 2016).

Chapter 2

Safety Standards and Methods of Reliability Assessment[*]

Chapter 1 presented an overview of safety systems of escalators, elevators and moving walks, and identified that, in order to maintain reliability, redundancy and/or replacement of old mechanical components in these safety systems is required. Since reliability is one of the main criteria in making decisions for applying redundancy/replacement of components, it is necessary to have knowledge about available methods and related standards which can be used in reliability calculation of heterogeneous safety systems.

Functional safety standards propose formulas for the calculation of PFD_{avg}/PFH (Average Probability of Dangerous Failure on Demand/Average Frequency of Dangerous Failure per Hour) which numerical values are used for establishing correspondence to the SIL (safety integrity level). The international standards IEC 61508 (general functional safety standard) and ISO 22201-2 (safety standard specified for escalators and moving walks) have special requirements with respect to a SIL. All systems and subsystems of these machines should correspond to the required SIL. However the analytical formulas of reliability calculation suggested in these standards cannot be used for heterogeneous redundant systems with a combination of mechanical, electronic/electrical components and constant and non-constant failure rates. Methods of reliability assessment are not always applicable to heterogeneous safety systems. Therefore this Chapter presents an overview of the existing safety standards, reliability assessment methods, and shows their application area, benefits, drawbacks and limitations.

[*] This chapter is based on E. Rogova, G. Lodewijks, Y. Pang (2014);
E. Rogova, G. Lodewijks (2016).

Section 2.1 contains an overview of standards that are used for reliability prognosis of a braking system of moving walks. Section 2.2 presents methods of reliability assessment of heterogeneous M-out-of-N redundant safety systems.

2.1 Standards in reliability prognosis of braking system of moving walks

There are many safety standards that regulate norms of construction, exploitation and functional safety of equipment in different engineering fields. These standards have requirements, recommendations, methods and tools for a reliability analysis. Although safety and reliability are different properties, and a system can be reliable but unsafe and vice versa (Leveson, 2011), surely, safety and reliability are closely related. For moving walks it is assumed in this study that unreliable subsystems cannot be safe. That is why the system has to be reliable and to meet requirements of related standards and norms. Reliability is defined as “ability of a functional unit to perform a required function under given conditions for a given time interval”. “The term used in IEV 191-02-06 is “reliability performance” and the definition is the same with additional notes” (ISO/IEC 2382-14, 1997). Prediction of the reliability value not only for a specified time period, but also for the whole exploitation period of a system is called reliability prognosis.

The role of a reliability prognosis cannot be overestimated, especially for degrading components/subsystems. Reliability prognosis plays a serious role in maintenance management of a machine. “The ability to forecast machinery failure is vital to reducing maintenance cost, operation downtime or operation risk” (Sun and Jia, 2011). Reliability prognosis of the machine consists of several parameters: 1) prediction of time to failure of the machine; 2) estimation of money expenditure for future repair; 3) planning of an appropriate repair or replacement of equipment to reduce the cost of major repairs. Such prognosis allows to reduce probability of accidents and money expenditure for repair of equipment. Reliability prognosis is used in different engineering fields such as nuclear, chemical, aerospace, civil and other fields. This section is focused on implementation of reliability prognosis of a braking system of moving walks.

In most cases reliability prognosis is executed due to degradation of parts of the system. The fundamental challenge when we introduce the non-constant failure rate is related to the degradation. This means that even if the failures have been repaired during the proof test, the system cannot be considered as good as new: PFD_{avg} after every test interval is higher than PFD_{avg} for the previous test interval. This is the main challenge that has to be taken into account. Therefore the reliability prognosis is especially important for systems with non-constant failure rates.

In literature four main groups of prognostic approaches for degradation systems are described: experience-based, model-based, knowledge-based and data-driven (Gojian et al., 2009). In practice, a reliability prognosis of complex systems does not use only one method; sometimes engineers apply even a few approaches. The type of reliability prognosis depends on the nature of degradation. For instance, some components such as controllers do not have degradation during the exploitation period. They have an approximately constant failure rate. But others (mechanical components) have strong degradation of reliability parameters. Reliability degradation of a braking system of moving walks is caused by wear of mechanical and hydraulic components. Combination of experience-based, SIL-based approach and application of international standards is used here as a tool for reliability prognosis of a braking system of moving walks. This combined method enables estimation of the overall reliability of a system, and also can announce not appropriate safety integrity level in advance.

The method described here for the reliability analysis and prognosis is SIL-based which means using the SIL concept - the central concept of functional safety, described in the standard IEC 61508 “Functional safety of electrical/electronic/programmable electronic safety-related systems”. The safety integrity level is defined as “a discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems” (IEC 61511-1, 2004). The standard ISO 22201-2 “Programmable electronic systems in safety related applications — Part 2: Escalators and moving walks (PESSRAE)” specifies general requirements of IEC 61508 for escalators and moving walks (ISO 22201-2, 2013). These and other standards establish requirements for functional safety of moving walks. However, SIL-based reliability analysis and prognosis of a braking system of moving walks were not considered in research until now. Meanwhile this approach allows not only meeting all requirements of related standards, it also allows creating a suitable tool for engineers, constructors and audit companies. Section 2.1.1 proposes using related standards in different stages of reliability prognosis of a braking system of moving walks.

2.1.1 Interaction of standards

There are several safety standards for consideration of safety questions of moving walks. They can be divided into four groups:

1) standards of functional safety (IEC 61508, IEC 62061, ISO 22201-2, ISO 13849-1);
2) reliability analysis tools (IEC 60300-3-1, IEC 61649, IEC 61078, IEC 61165 etc.);
3) risk assessment (ISO 14798, ISO 12100, ISO/TR 14121-2);
4) mechanical safety standards for the sector application (EN115-1+A1, ISO 18738-2).

A diagram of the standards interaction is shown in Figure 2.1. All four groups of standards are correlated to each other and used for reliability prognosis of moving walks. Moreover, all these standards should be studied in a complex reliability analysis of a braking system of moving walks.

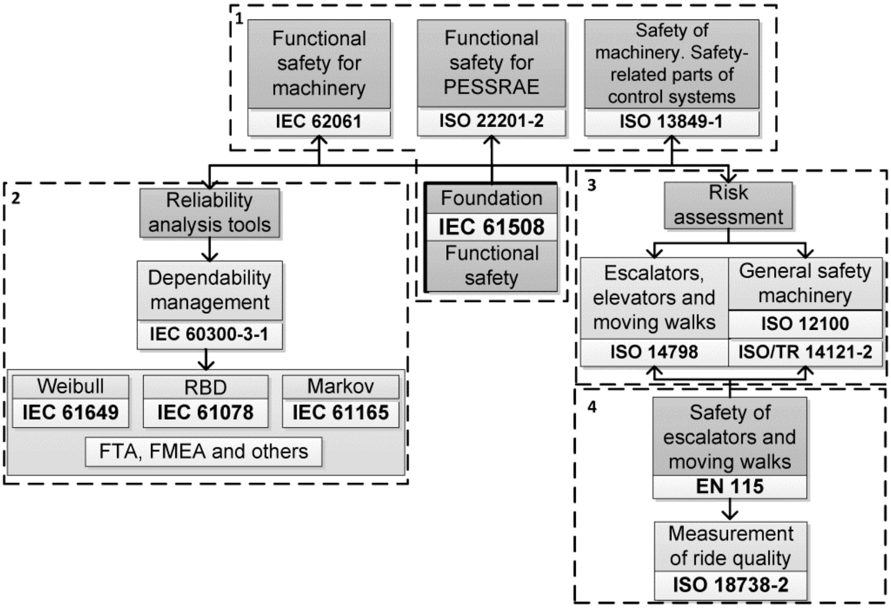


Figure 2.1: Diagram of standards.

These groups of standards are used in different stages of reliability prognosis. The standards from the third group can be used mainly in the determination of safety requirements stage. The standards from the second group are used in the stage of reliability analysis in accordance to safety requirements. The fourth group provides information for the development of additional safety devices, diagnostic systems and redundancy architecture on the stage of reliability improvement. The first group gives general requirements and recommendations in accordance to the functional safety concept. Standards from this group are used in all the stages of analysis as a main guideline. Figure 2.1 proposes the general scheme of interactions of standards. These four groups of standards can be supplemented with other standards. For example the standard IEC 61882 for HAZOP (hazard and operability) analysis can be added to the third group of standards for some applications.

Safety standards such as IEC 61508 from the first group of standards are an important source of information for development of safety-critical systems in many engineering fields, including transport engineering. IEC 61508 has become a foundation of international standards for safety-related systems such as airborne systems, railway, nuclear power plants, medical equipment, energy and process systems, machinery, furnaces and automobiles (Azianti, 2013). IEC 61508 defines general safety integrity requirements for safety functions allocated to the E/E/PE safety-related systems: SIL1 is the lowest level, SIL4 is the highest. However, IEC 61508 “does not specify the safety integrity levels required for sector applications (which must be based on detailed information and knowledge of the sector application). The technical committees responsible for the specific application sectors shall specify, where appropriate, the safety integrity levels in the application sector standards” (IEC 61508-1, 2010). This standard does not provide engineers with specific requirements and recommendations for development of transport equipment. That is why three standards of functional safety of machinery were developed: IEC 62061, ISO 22201-2, and ISO 13849-1. IEC 62061 provides a machine sector with a specific framework for functional safety of machines in general (IEC 62061, 2005). ISO 22201-2 has been developed “in order that consistent technical and performance requirements and rational be specified for Programmable Electronic System in Safety-Related Application for Escalators and moving walks (PESSRAE)” (ISO 22201-2, 2013). This standard is based on IEC 61508, IEC 62061, and EN 115-1, and is considered as an “application sector standard”

(IEC 61508-1, 2010). However, ISO 22201-2 defines risk classes by means of the table with correspondence between frequency of accidents and risk consequences. There are no guidelines or rules in this standard how to transfer from risk classes to SILs. The standard defines the highest (SIL3) and the lowest (SIL1) possible safety integrity levels for moving walks. ISO 13849-1 from the first group of standards provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems of machinery (ISO 13849-1, 2008).

The third group of standards is divided into two subgroups: general risk assessment for safety machinery and risk assessment for escalators, elevators and moving walks. The standard ISO 14798 "Lifts (elevators), escalators and moving walks - Risk assessment and reduction methodology" describes examples of hazards, principles and set procedures of risk assessment for elevators, escalators and moving walks (ISO 14798, 2009). Unfortunately, ISO 14798 and ISO 22201-2 do not explain how to define accident consequences.

The standard ISO 12100 (Safety of machinery - General principles for design - Risk assessment and risk reduction) is a basic safety standard "giving basic concepts, principles for design and general aspects that can be applied to machinery" (ISO 12100, 2010). This standard describes procedures for identifying hazards and estimating and evaluating risks during relevant phases of the machine life cycle, and for the elimination of hazards or the provision of sufficient risk reduction. "The practical use of a number of methods for each stage of risk assessment is described in ISO/TR 14121-2" (ISO 12100, 2010).

The technical report ISO/TR 22100-2 describes how ISO 12100 relates to ISO 13849-1 from the first group of standards. "For the correct application of ISO 13849-1, basic input information resulting from the application of the overall risk assessment and risk reduction process for the particular machine design is necessary. Based on this input information, the safety-related parts of the control system can be appropriately designed according to ISO 13849-1. Information resulting from a detailed design of safety-related parts of the control system relevant for its integration into the machine design has then to be considered in the overall risk assessment and risk reduction process according to ISO 12100" (ISO/TR 22100-2, 2013).

The standards from the fourth group contain mechanical data for safety limitations. EN 115-1+A1 comprises all types of hazards, allowable distances, speed and load limitations etc (EN 115-1, 2010). ISO 18738-2 provides readers with information about ride quality of escalators and moving walks, it is focused mainly on vibration and noise.

The second group of standards is used for reliability analysis. In accordance to the functional safety approach, after determination of SIL assigned for the safety function, it is required to conduct reliability analysis of the safety system. The standard IEC 60300-3-1 describes dependability techniques, their advantages and disadvantages, data input and other conditions for using various techniques (IEC 60300-3-1, 2003). Standards IEC 61649 (Weibull analysis), IEC 61078 (Analysis techniques for dependability – Reliability block diagram and boolean methods), and IEC 61165 (Application of Markov techniques) describe their methods which can be applied for reliability analysis and prognosis of a braking system of moving walks.

Reliability analysis methods can be divided into two main groups: qualitative and quantitative. Qualitative reliability analysis methods are used for analysis of the functional system structure, determination of "system and component fault modes, failure mechanisms, causes, effects and consequences of failures" (IEC 60300-3-1, 2003). Qualitative methods cannot estimate numerical values of reliability. Three most widely used methods of quantitative reliability analysis are presented in Figure 2.1: Fault tree analysis (FTA), Reliability Block Diagram (RBD), and Markov analysis (MA). These methods are used for reliability assessment of different architectures and complexity of safety systems. Very often combination of qualitative and quantitative methods is used for reliability assessment of a safety system.

Markov analysis considers all possible states of a system. This method is mainly used for systems with constant failure rates (IEC 61165, 2006). Markov state diagram allows to obtain a system of Kolmogorov differential equations. Solving the system of equations gives values of state probabilities. A braking system contains electronic components with constant failure rates, and mechanical with non-constant failure rates. Therefore conventional MA is not appropriate for an overall reliability analysis of a braking system of moving walks or can be applied partially to some subsystems.

FTA as well as RBD are related to one of the top-down methods. These methods are able to account for effects arising from a combination of faults (IEC 60300-3-1, 2003). As IEC 60300-3-1 states, RBD is applicable for non-repairable systems "where independent blocks can be assumed" (IEC 60300-3-1, 2003).

Analytical formulas suggested by the standards cannot be used for systems with non-constant failure rates. The standard IEC 61649 helps in modelling degradation of mechanical components with non-constant failure rates by using Weibull distribution (IEC 61649, 2008). However, different architectures of systems with failure rate functions modeled by Weibull distribution, require different methods of reliability assessment.

The problem of reliability assessment of heterogeneous safety systems with non-constant failure rates is not limited by moving walks, escalators and elevators. This problem is much wider and covers many other safety systems/equipment that contain degrading components. As was shown in this section, safety standards are not always able to give a required formula for reliability assessment. Therefore the next Section considers methods of reliability assessment methods for complex architectures with non-constant failure rates and particularly heterogeneous redundant safety systems.

2.2 Methods of reliability assessment of heterogeneous M-out-of-N redundant systems

2.2.1 Different architectures

As was mentioned before, standards IEC 61508, 61511 and 62061 describe in details the procedure of reliability assessment of SIS (safety instrumented system) for the determination of the corresponding SIL (IEC 61511-1, 2004; IEC 62061, 2005; IEC 61508-1, 2010). Analytical formulas for calculating PFD_{avg} and PFH values for systems with M-out-of-N architecture are presented in book 6 of IEC 61508 (IEC 61508-6, 2010). However these formulas can be used only if the failure rates of a system are constant and channels are identical. For heterogeneous redundancy that is defined as mixing of different types of components (Sharma et al., 2011) with different channels and combination of constant and non-constant failure rates, it is necessary to apply other methods.

The main feature of heterogeneous redundant systems is the existence of different types of components. There are many different components that can be used in such systems from the level of sensors and detectors till the level of actuators and mechanisms. From the reliability point, components are divided into two categories:

1. The first category is based on the nature of component: mechanical or electrical/electronic.
2. The second category is a consequence of the first one: constant (λ) or non-constant (z(t)) failure rates.

It is also important to clarify the identity or difference of channels in redundancy architecture:

a. different components are located in the same channel, but all channels are identical;
b. channels are also different.

The choice of constant or non-constant failure rate in the second category depends on many parameters. First of all it depends on the available information for the specific component and approximation on the basis of a chosen model. Mechanical and electrical/electronic components have different physical principles. Many mechanical components have degradation of their reliability parameters that means non-constant failure rates. Electronic/electrical components also can have degradation. However the majority of them are assumed to have approximately constant failure rates.

Figure 2.2 demonstrates different types of M-out-of-N architecture. Case a) is an M-out-of-N architecture with different channels and constant failure rates. The problem of reliability assessment of such heterogeneous redundant architecture can be solved by using a reliability block diagram (RBD) and all other methods that work with constant failure rates. Case b) is a homogeneous redundant system: it has identical channels. The failure rates of each channel in this architecture are identical, but not constant: this requires methods that will be able to work with non-constant failure rates. It should here be noted that some methods applicable for the case b) work only for systems with one component level redundancy and cannot be used for systems with several different components in one channel. Case d) represents the case of different channels and different non-constant failure rates. Case c) is the most difficult case due to different channels and a combination of constant and non-constant failure rates.

In general reliability assessment methods for heterogeneous redundant systems have two main issues: 1) non-identical channels and 2) non-constant failure rates. It is not difficult to find methods for each of these issues separately. However there are no practical methods that are able to cope with both of these issues simultaneously if the system is repairable.

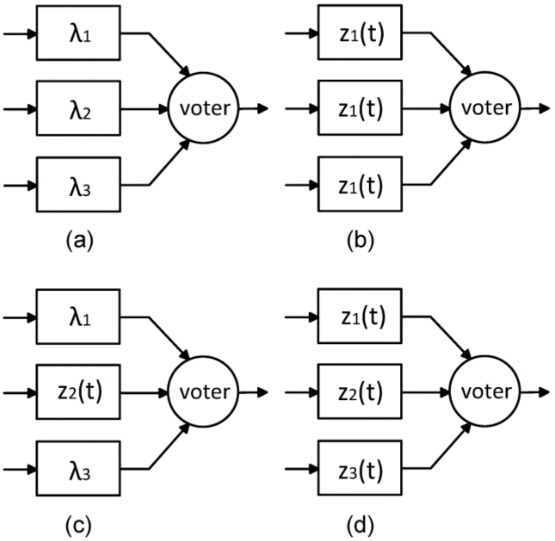


Figure 2.2: Heterogeneous redundant systems.

2.2.2 Constant or non-constant failure rates

Degradation of mechanical components is a natural process that occurs with hydraulic, pneumatic, electro-mechanical, mechanical equipment in the wear-out region. The well-known bathtub curve model demonstrates the life of the component by three regions: 1) Burn in (infant mortality); 2) Useful life (constant failure rate); 3) Degradation (wear out). As shown in Figure 2.3, duration of the useful life region can be very different. For example, for electronic components useful life is the largest region of the bath tube curve, and they rarely have a wear-out region. However for mechanical components this region can be very short. Very often start of degradation depends on operating conditions. Many mechanical components have degradation over time that means non-constant failure rates. However sometimes it is not easy to obtain a failure rate function and to find an appropriate reliability method. In some cases non-constant failure rates can be assumed as approximately constant under specific conditions.

Alfredsson and Waak (Alfredsson and Waak, 2001) compare constant and non-constant failure rates. The authors separate constant demand rates and constant components rates. They assume constant demand rates without assuming constant component failure rates. The reason of this assumption is that “the demand process for a given item type at a given site is the result (in essence the superposition) of a number of component failure processes”. In this case, the demand process can be approximated by a Poisson process, that means the demand rate is approximately constant (Alfredsson and Waak, 2001). Jones (Jones, 2001) considers a failure intensity analysis for estimation of system reliability using a non-constant failure rate model. He conducts an analysis of failure intensity curve of CMOS digital integrated circuits with 1000 hour intervals. The shape of the curve obtained by Jones is “ample evidence that the constant failure rate assumption for this type of device is incorrect” (Jones, 2001). It is also important to notice that Jones considers only the first part of the bath-tube curve by using an example of CMOS digital devices. For mechanical components the last region of the bath-tube curve is mainly of interest (Figure 2.3). This region is related to the degradation process.

For obtaining a failure rate function it is necessary to choose an appropriate distribution that can describe a degradation process. There are different distributions that can be chosen. However, many researchers and practitioners use a Weibull distribution for the mathematical description of the wear out failure characteristics (Chudoba, 2011; Kumar and Jackson, 2009; Keller and Giblin, 1985). A failure rate function of two-parameter Weibull distribution is demonstrated in Equation 2.1:

$$z(t) = \frac{\alpha \cdot t^{\alpha-1}}{\eta^{\alpha}} \tag{2.1}$$

where α – Weibull shape parameter; η – Weibull scale parameter.

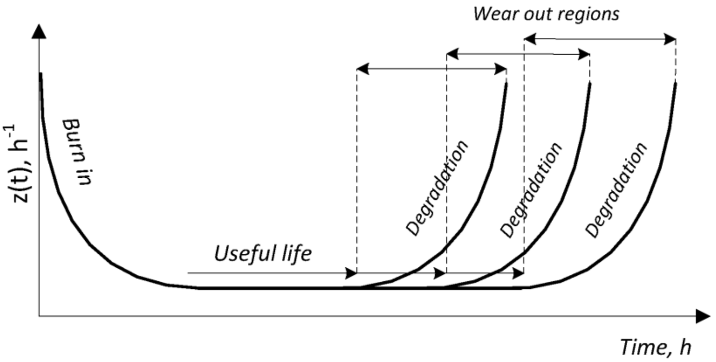


Figure 2.3: Bathtub curve.

Weibull shape and scale parameters can be obtained from real statistical data and also from Weibull databases where values of α and η are presented for typical components (Barringer & Associates, Inc., 2010). These databases are very helpful if real statistical data is not available. However such data from databases should be used with caution because they give very approximate average values for components. Weibull parameters for the same components, which are produced by different manufacturers or have different operating conditions, can be very different.

Constant failure rates can be applied as an approximate solution for components with non-constant failure rates if the following condition is met: the difference in values of the failure rate at the beginning and at the end of the interval is not significant. This means that the calculated PFD_{avg}/PFH values of a system at the beginning and at the end of the interval should correspond to the same SIL. As a consequence of this condition, the test interval, “the elapsed time between the initiation of identical tests on the same sensor, channel, etc.” (IEEE Std. 352, 1985), has to be chosen properly in accordance to the recommendations given by functional safety standards and Rausand and Hoyland (Rausand and Hoyland, 2004).

It is important to understand that SIL-requirements for a safety system are the same for the whole test interval and in case of neglecting significant changes of failure rates, calculated values of PFD_{avg} and PFH may be much lower than the real values. For low-demand safety systems the proof-test interval is usually in the order of 6 months to 2-3 years (Rausand and Hoyland, 2004). Some test intervals can be too large for an approximation by a constant failure rate in case of degrading systems. Failure rates for some mechanical components obtained by using Weibull data bases and Equation 2.1 are presented in Table 2.1:

Table 2.1: Failure rate values for mechanical components (Rogova et al., 2015).

Failure rate	Solenoid valve	Gears	Bearings
z(t=1h)≠const	$2.13\cdot10^{-4}$	$8.27\cdot10^{-5}$	$3.86\cdot10^{-4}$
z(t=8760h) ≠const	$5.29\cdot10^{-4}$	$1.18\cdot10^{-1}$	$1.00\cdot10^{-3}$
z_{avg}(t=8760h)=const	$3.71\cdot10^{-4}$	$9.0\cdot10^{-2}$	$6.93\cdot10^{-4}$

As Table 2.1 shows, the non-constant failure rate of a solenoid valve can be approximated as a constant failure rate z_{avg} because the difference of values at the beginning and at the end of the test interval is negligible. However difference of failure rate values for gears at the beginning and at the end of the test interval is very large and the failure rate function cannot be replaced by constant value. The difference between values of failure rates of bearings at the beginning and at the end of the test interval is larger than for Solenoid valve. This change of failure rate should be considered taking into account a correspondence to the required SIL at the beginning and at the end of the test interval to take a decision about possibility to make an approximation by constant failure rate. This method of correspondence to SIL is applicable for all components (solenoid valve, gears, bearings and others) but especially useful in those cases when approximation by constant failure rate is not obvious.

It is also important to notice that non-constant failure rates allow to make a valuable reliability prognosis of equipment. It can help in maintenance scheduling. For example if a compressor is one of the most critical components of a safety system, it is very important to follow the degradation and to build a failure rate function that can help in calculating the PFD_{avg}/PFH values and determination of the corresponding safety integrity level (SIL) of a system. The example of such measurements of vibration rate in compressor is shown in Table 2.2.

Table 2.2: Increase of vibration rate of compressor.

Weeks, No	1	2	3	4	5
Vibration rate, mm/s	0.8	1	1.3	1.8	2.6

For the purpose of reliability prognosis, the compressor is tested every week. Based on the failure rate function obtained from these measurements, it is possible to conclude that for example after N weeks of exploitation, SIL of safety system that contains the compressor will not correspond to the required SIL. This means it is necessary to plan maintenance before appearance of critical vibration. The similar measurements can be conducted for other mechanical equipment of heterogeneous M-out-of-N redundancy architecture where such periodical measurements (like partial stroke tests for example) are a part of diagnostics.

2.2.3 Overview of reliability assessment methods

In this section different methods are considered that can be applied for the reliability assessment of different types of heterogeneous redundant systems. In addition some possibilities to avoid excessive complexity are demonstrated. Analytical formulas and algorithms suggested by these methods, can be used in different safety systems at the design stage to suit the required SIL. It is also important for the determination of a repair/maintenance policy.

The methods of reliability assessment of heterogeneous M-out-of-N redundancy architectures are presented in Figure 2.4. These methods are grouped in accordance to the classification introduced in Section 2.2.1 (Figure 2.2). Each case (a, b, c, d) has a set of methods that are applicable for the reliability assessment of corresponding architectures.

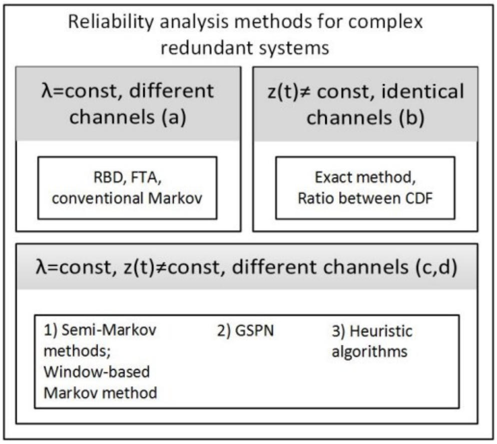

Reliability analysis methods for complex redundant systems
λ=const, different channels (a)
RBD, FTA, conventional Markov
z(t)≠ const, identical channels (b)
Exact method, Ratio between CDF
λ=const, z(t)≠const, different channels (c,d)
1) Semi-Markov methods; Window-based Markov method
2) GSPN
3) Heuristic algorithms

Figure 2.4: Reliability assessment for complex redundant systems.

Reliability analysis for Case a) non-repairable systems can be easily solved by using a Reliability Block Diagram (RBD), a Fault Tree Analysis (FTA). Conventional Markov method can be used for Case a) repairable systems. For example, Hildebrandt (Hildebrandt, 2007) applies a conventional Markov model for the calculation of the PFD value for a heterogeneous 1oo2 architecture. Case b) is more difficult. Here for the calculation of the PFD$_{avg}$ value of M-out-of-N non-repairable systems the “exact method” (Rausand and Hoyland, 2004) can be used. It is based on the definition of PFD$_{avg}$:

$$\begin{cases} PFD_{MooN} = 1 - \frac{1}{\tau}\int_0^{\tau} R_{MooN}(t)dt \\ R_{MooN} = \left(\sum_{i=M}^{N}\binom{N}{i}R^i \cdot (1-R)^{N-i}\right) \cdot R_{CCF} \\ \quad = \left(\sum_{i=M}^{N}\binom{N}{i}e^{-\frac{(1-\beta)z_{DU}(t)\cdot t\cdot i}{\alpha}} \cdot \left(1 - e^{-\frac{(1-\beta)z_{DU}(t)\cdot t}{\alpha}}\right)^{N-i}\right) \cdot e^{-\beta z_{DU}(t)\cdot t} \end{cases} \tag{2.2}$$

where R_{MooN} is system reliability, calculated by using a Weibull distribution;
R is reliability of one channel;
$z_{DU}(t)$ is a failure rate function of dangerous undetected failures (DU);
β is a CCF (Common Cause Failures) factor.

The method for calculation of PFH values which is based on the definition of PFH also allows to obtain result for the case b):

$$PFH = \binom{N}{N-M+1} \cdot \left(\frac{(1-\beta)\cdot z_D(\tau)}{\alpha}\right)^{(N-M+1)} \cdot \tau^{N-M} + \frac{\beta\cdot z_D(\tau)}{\alpha} \tag{2.3}$$

The exact method of PFD$_{avg}$ calculation is simple and transparent. However analytical calculation of the integral is impossible if the failure rate function is described by a Weibull distribution. In this case the method requires calculation of an approximate numerical solution that is not always suitable due to the accuracy of the results.

The alternative method “Ratio between CDFs” (which will be presented in Chapter 4 in more details) also can be used for reliability analysis of an M-out-of-N redundancy architecture with identical channels and non-constant failure rates (case b). Therefore the PFD$_{avg}$ for the first test interval k$_1$ (Rogova et al., 2015):

$$PFD_{avg,k_1} \approx \binom{N}{N-M+1} \cdot \frac{A_k}{\alpha+1}\left(\frac{(1-\beta)z_{DU}(\tau)\cdot\tau}{\alpha}\right)^k + \frac{\beta z_{DU}(\tau)\cdot\tau}{\alpha(\alpha+1)}$$
$$A_k = \left[\sum_{i=1}^{k}\sum_{l=0}^{k-i}\binom{k}{i}\binom{k-i}{l}\ (-1)^l \cdot \frac{1}{(i+l)}\right]^{-\alpha} \quad (2.4)$$

where k=N-M+1; τ – test interval; A_k is a "multiplier" which depends only on k and the Weibull shape parameter. The method also proposes a formula for PFD_{avg} prognosis:

$$PFD_{avg,ki} = \binom{N}{N-M+1}\frac{A_k}{(1+\alpha)}\left(\frac{(1-\beta)\cdot z_{DU}(\tau)\cdot\tau}{\alpha}\right)^k \cdot [i^{\alpha+1}-(i-1)^{\alpha+1}] \cdot$$
$$[i^{\alpha}-(i-1)^{\alpha}]^{k-1} + \frac{\beta z_{DU}(\tau)\cdot\tau}{\alpha(\alpha+1)} \cdot [i^{\alpha+1}-(i-1)^{\alpha+1}] \quad (2.5)$$

where i – is a number of test interval τ.

The main limitation of the method "Ratio between CDFs" is the component level redundancy. For example if there are several components in one channel, this method cannot be applied: the method uses Weibull shape and scale parameters of a component in one channel. However, this method can be used if Weibull parameters were estimated for the whole channel in general, but not for each component of a channel separately.

Cases c) and d) are the most difficult ones because they combine two main issues: non-constant failure rates and non-identical channels. Markov and GSPN methods are applicable to architectures c) and d) also in case of repairable systems. The first solution is Markov-methods. The conventional Markov method is not applicable because conclusions about exponential distribution of corresponding time intervals for systems with non-constant failure rates are unjustified (Harlamov, 2008). However semi-Markov methods are able to cope with this problem. "The main advantage of semi-Markov processes is to allow non-exponential distributions for transitions between states and to generalize several kinds of stochastic processes. Since in most real cases the lifetime and repair time are not exponential, this is very important" (Limnios and Oprisan, 2001). For example, Kumar et al. (Kumar et al., 2013) consider a steady-state semi-Markov method for calculation of availability of repairable mechanical systems. A steady-state semi-Markov method suggests a solution by using an assumption that state probabilities are not changing. This assumption is not always applicable. That is the reason why the method can only be accepted with caution. A steady-state Markov method starts from the state-diagram where CDFs (Cumulative Distribution Functions) are assigned for each transition instead of failure rates. Based on known CDFs it is possible to build a kernel matrix $Q(t)^{[PxP]}$ (P – is a number of states), which elements together with sojourn times, the amount of time that the system spends while being at the state before jumping to another state (Ibe, 2013), are used for calculating state probabilities. At the final stage of this method, PFD_{avg} and PFH values can be easily calculated based on values of steady-state probabilities. The steady-state method is time-consuming and is not applicable for transient analysis but it can be used as an additional method for comparison of obtained results.

In the case of complex semi-Markov models, calculating the exact probability distribution of the first passage time to the subset of states is usually very difficult. Therefore, the only way is to find an approximate probability distribution of that random variable. This is possible by using the results from the theory of semi-Markov processes (SMP) perturbations. The perturbed SMPs are defined in different way by different authors (Grabski, 2014). There are significant results presented by Korolyuk and Turbin (Korolyuk and Turbin, 1976), Gertsbakh (Gertsbakh, 1984), Pavlov and Ushakov (Pavlov and Ushakov, 1978) and others. The difference of this method in comparison to conventional and semi-Markov method is clear from the beginning: at the stage of definition of system states. The space of K states should be divided into two subspaces: subspace A`={0,..,j} when the system is "up" and subspace A={j,..,K} when the system is "down". As a result this method allows to obtain an approximate reliability function R(t) (Grabski, 2014). However solving complex matrix equations and other time-consuming calculations make this method difficult for application in practice. In addition, this method is applicable only if all conditions of the corresponding theorems are met. Obtained results are approximate and require comparison with other methods.

Taking into account all mentioned problems related to the usage of semi-Markov method, the new window-based Markov method was developed in this dissertation and presented in Chapter 5. This method allows to work with architectures c),d). It is simple from the stage of modelling till the stage of finding a numerical solution.

There are methods that are based on heuristic algorithms. For example Boddu and Xing consider the reliability of non-repairable M-out-of-N redundancy architecture with mixed spare types for different redundancy modes: hot, cold, mixed (Boddu and Xing, 2012). Li and Ding presented research about optimal allocation policy of active redundancies to M-out-of-N systems with heterogeneous components (Li and Ding, 2010). The question of reliability estimation of heterogeneous multi-state series-parallel systems was considered by Sharma et al. (Sharma et al., 2011) and Wang and Li (Wang and Li, 2012). However, these papers are mainly focused on existing heuristic algorithms and some difficulties related to optimization problems and do not aim at a practical calculation of system reliability in the concept of functional safety.

GSPN (Generalized Stochastic Petri Nets) also can be used for calculation reliability in cases c)-d). This method was described for instance by Santos et al. (Santos et al., 2014). The authors use the GSPN model for an estimation of the system age and a Weibull failure rate function for the failure rate function. Dersin et al. (Dersin et al., 2008) use a Petri-nets approach for maintenance modelling. GSPN is one of the most complex and time-consuming methods for reliability assessment of architectures c)-d). It requires a high level of special knowledge and it is not easy to build a model. Markov methods are easier at the stage of model building. Often GSPN is used in a combination with Monte Carlo simulation (MCS).

Monte Carlo simulation is not shown in Figure 2.4. However MCS is used as a part of many methods very often. It is also used for comparison and verification of the results obtained by using other methods. The main algorithm of MCS is in the discretization of the problem of calculation of state probabilities: the test interval [0;τ] should be splitted into intervals with duration h. Thus the reformulated problem is the problem of defining of state probabilities at discrete moments of time: $P_i((j-1)h)$.The main principles of MCS with application in reliability theory are described by E. Zio (Zio, 2013).

2.2.4 In practice

The purpose of applying redundancy is the increase of reliability. “The capabilities of M-out-of-N redundancy make it an important tool for failure prevention. Sometimes components are deliberately subdivided in order to permit M-out-of-N redundancy to be applied” (Hecht, 2004). Practical implementation of M-out-of-N heterogeneous redundancy architectures, which types are demonstrated in Section 2.2.1, is very wide. Case a) (see Figure 2.2) is frequent in safety systems: very often the same type of components are not totally identical and produced by different manufacturers. Moreover, as was discussed in the Introduction, this non-identity is recommended by the standards (IEC 61508-6, 2010; IEC 62061, 2005) to decrease CCF. Cases b)-d) are devoted to mechanical components in channels. Architecture b) can be not very reliable because of identical mechanical equipment in its channels. This type of redundancy gives a high probability of common cause failures and less probability to diagnose possible dangerous failures. Case d) is much better in terms of reliability due to hardware diversity. A practical example of case c) is existence of different types of relays in different channels: electro-mechanical relays with degradation and electronic solid-state relay (SSR) with constant failure rates. The type of heterogeneous redundancy demonstrated in case c) is very interesting for application in safety systems because the existence of components with different physical principals allow to reach a high reliability.

As was discussed in Section 2.2.3, complex methods of reliability assessment are applied to the parts of large engineering systems because many of these methods are not able to calculate the reliability of a system with thousands of components and hundreds of subsystems. These methods are basically applied to some critical subsystems, and the obtained results are used in further work for investigation the reliability/availability of a system in general.

To start a reliability analysis of complex systems with heterogeneous subsystems (including M-out-of-N redundancy architectures), it is necessary to start from a general investigation of the system. If reliability analysis of such large systems is performed on the stage of exploitation (but not at the design stage), it is useful to focus on existing statistics of failures. In this case it is possible to use a qualitative FTA (fault tree analysis) (Rausand, 2014) or FMECA (Failure mode, effects and criticality analysis) (Rausand and Hoyland, 2004) for example. These tools will help in understanding the weakest points of a safety system from the reliability point of view. This understanding will allow to focus on specific subsystems for a detailed analysis by using methods described in Section 2.2.3. In accordance to the functional safety approach, the main purpose of a reliability assessment of critical degrading subsystems is checking of correspondence of SIL of safety system to the required SIL of safety function that is performed by safety system (IEC 61508-1, 2010).

Application of safety standards and using of SIL-based methodology, described in these standards, simplifies not only the work of audit companies. Using a unified procedure also helps engineer-constructors, project managers at the design and maintenance stages. Safety integrity levels of all the safety functions should be defined in accordance to IEC 61508. Depending on the complexity of a system, there are one, two, three or many subsystems, which perform safety functions. Equipment for these subsystems should correspond to appropriate safety requirements. Knowledge of SIL assigned for a safety function, allows to calculate SIL of safety system which performs this safety function. It gives a possibility to find suitable equipment at the design stage of moving walks. It means that a project manager has to buy, for example, 5 devices with SIL2, SIL2, SIL3, SIL3 and SIL2 respectively to provide a safety function of SIL2.

2.3 Conclusions

This Chapter presented the overview of safety standards (Figure 2.1) for moving walks and escalators, and methods (Figure 2.4) that are used for the reliability assessment of redundant safety systems. The results of this overview are presented as follows:

1. The methodology described in the safety standards gives general guidelines from risk assessment and determination of the SIL requirements till reliability analysis and reliability enhancement. These safety standards do not have analytical formulas of reliability assessment that are applicable for safety systems with non-constant failure rates.
2. Such analytical methods like RBD, Markov analysis, exact method, can be used for reliability assessment of redundancy architecture with identical channels and constant failure rates.
3. A few analytical methods of reliability assessment are available for systems with identical channels and non-constant failure rates: the exact method and analytical formulas of the “ratio between CDFs”.
4. Heterogeneous redundancy with different channels and a combination of constant and non-constant failure rates does not have analytical formulas of reliability assessment. Methods of reliability assessment that can be used

for this type of architecture are mainly simulation. Petri Nets are applicable for this type of architecture. However it is a time-consuming complex method that is often used together with Monte Carlo simulation.

5. This Chapter presented an answer to the first research question: *Which methods and safety standards are available for reliability assessment of redundant safety systems?* A lack of analytical methods of reliability assessment for heterogeneous redundant systems with different channels and a combination of constant and non-constant failure rates was revealed.

Application of methods of reliability assessment described in this Chapter, will be presented in Chapter 3 on the example of a braking system of moving walks. The criterion of applying redundancy of a braking system of moving walks will be explained by using the functional safety concept presented in this Chapter.

References

Alfredsson, P., Waak, O. (2001) *Constant vs. Non-Constant Failure Rates: Some Misconceptions with respect to Practical Applications*, Systecon, Stockholm.

Azianti, I. and Won, J. (2013) Research Trends in Automotive Functional Safety, *2013 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE); Proc. intern. conf., Emeishan, Sichuan, China, 15-18 July 2013.* IEEE.

Barringer & Associates Inc. (2010) *Weibull Database*. Available at: http://www.barringer1.com/wdbase.htm (Accessed 17 February 2014).

Boddu, P. and Xing, L. (2012) Redundancy Allocation for k-out-of-n: G Systems with Mixed Spare Types. Proc. *Reliability and Maintainability Symposium (RAMS)*, Reno, NV, pp.1-6.

Chudoba, J. (2011) Modelling of dynamical dependability by using stochastic processes. Proc. *European Safety and Reliability conference (ESREL)*, Troyes, France, 2045-2049.

Dersin, P., Péronne, A., Arroum, C. (2008) Selecting test and maintenance strategies to achieve availability target with lowest life-cycle cost. Proc. *Reliability and Maintainability Symposium (RAMS)*, Las Vegas, NV, USA, pp. 301-306.

European Committee for Standardization (CEN) (2010) *EN 115-1+A1. Safety of escalators and moving walks – Part1: Construction and installation.*

Gertsbakh, I.B. (1984) ‘Asymptotic methods in reliability theory: a review’, *Adv. Appl. Prob*, 16, pp.147–175.

Gojian, N. et al. (2009) A review on degradation models in reliability analysis, *the 4th World Congress on engineering asset management; Proc. intern. congr. Athens, Greece 28-30 September 2009.* Springer.

Grabski, F. (2014) *Semi-Markov Processes: Applications in System Reliability and Maintenance*. Chap.4, pp.67-82. Elsevier.

Harlamov, B. (2008) *Continuous Semi-Markov Processes.* Hoboken, NJ: John Wiley & Sons, Inc.

Hecht, H. (2004) *Systems Reliability and Failure Prevention*, Norwood, MA: Artech House, Inc.

Hildebrandt, A. (2007) Calculating the "Probability of Failure on Demand" (PFD) of complex structures by means of Markov Models. Proc. *4th European Conference on Electrical and Instrumentation Applications in the Petroleum & Chemical Industr*y, Paris, France, 1-5.

Ibe, O.C. (2013) *Markov Processes for Stochastic Modeling* (2nd edn). Waltham, MA: Elsevier, pp.50.

International Electrotechnical Commission (IEC) (2003) *IEC 60300-3-1. Dependability management Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology.*

International Electrotechnical Commission (IEC) (2004) *IEC 61511-1. Functional safety – Safety instrumented systems for the process industry sector. Part 1: Framework, definitions, system, hardware and software requirements.*

International Electrotechnical Commission (IEC) (2005) *IEC 62061. Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems.*

International Electrotechnical Commission (IEC) (2008) *IEC 61649. Weibull analysis.*

International Electrotechnical Commission (IEC) (2010) *IEC 61508-1. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1: General requirements.*

International Electrotechnical Commission (IEC) (2010) *IEC 61508-6. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3.*

International Organization for Standardization (ISO) (1997) *ISO/IEC 2382-14. Information technology - Vocabulary-Part 14: Reliability, maintainability and availability.*

International Organization for Standardization (ISO) (2008) *ISO 13849-1. Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design.*

International Organization for Standardization (ISO) (2009) *ISO 14798. Lifts (elevators), escalators and moving walks - Risk assessment and reduction methodology.*

International Organization for Standardization (ISO) (2010) *ISO 12100. Safety of machinery - General principles for design - Risk assessment and risk reduction.*

International Organization for Standardization (ISO) (2012) *ISO/TR 14121-2. Safety of machinery - Risk assessment - Part 2: Practical guidance and examples of methods.*

International Organization for Standardization (ISO) (2013) *ISO 22201-2. Lifts (elevators), escalators and moving walks – Programmable electronic systems in safety related applications – Part 2: Escalators and moving walks (PESSRAE).*

International Organization for Standardization (ISO) (2013) *ISO/TR 22100-2. Safety of machinery-Relationship with ISO 12100- Part 2: How ISO 12100 relates to ISO 13849-1.*

Jones, J. (2001) 'Estimation of System Reliability Using a "Non-Constant Failure Rate" Model'. *IEEE Transactions On Reliability*, 50 (3), pp.286-288.

Keller, A. Z., Giblin, M.T. (1985) Reliability Analysis of Commercial Vehicle Engines. *Reliability Engineering,* 10, pp.15-25.

Korolyuk, V.S. and Turbin, A.F. (1976) *Semi-Markov Processes and Their Applications*, Kiev: Naukova Dumka, (in Russian).

Kumar, G., Jain, V., Gandhi, O.P. (2013) 'Availability Analysis of Repairable Mechanical Systems Using Analytical Semi-Markov Approach'. *Quality Engineering*, 25(2), pp.97-107.

Kumar, R. and Jackson, A. (2009) Accurate reliability modeling using Markov analysis with non-constant hazard rates. Proc. *IEEE Aerospace conference*, Big Sky, MT, USA, pp. 1-7.

Leveson, N.G. (2011) *Engineering a safer world.* Cambridge, Massachusetts: The MIT Press.

Li, X. and Ding, W. (2010) 'Optimal Allocation Of Active Redundancies To k-out-of-n Systems With Heterogeneous Components'. *J. Appl. Prob*., 47, pp.254-263.

Limnios, N. and Oprisan, G. (2001) *Semi-Markov Processes and Reliability*. Birkhäuser, Boston.

Pavlov, I.V. and Ushakov, I.A. (1978) 'The asymptotic distribution of the time until a semi-Markov process gets out of the kernel', *Eng. Cybern,* 2(3), pp.68–72.

Rausand, M. (2014) *Reliability of Safety-Critical Systems: Theory and Applications*. John Wiley & Sons, Inc.: Hoboken, NJ.

Rausand, M. and Høyland, A. (2004) *System Reliability Theory. Models, Statistical Methods, and Applications* (2nd edn). Hoboken, NJ: John Wiley & Sons, Inc.

Rogova, E. and Lodewijks, G. (2016) Methods of reliability assessment of heterogeneous redundant systems. Proc. *8th IFAC Conference on Manufacturing*

Modelling, Management and Control MIM 2016, Troyes, France, IFAC-PapersOnLine, 49(12), pp.139–144.

Rogova, E., Lodewijks, G., Lundteigen, M.A. (2015) Analytical formulas of PFD calculation for systems with non-constant failure rates. Proc. *European Safety and Reliability conference (ESREL)*, Zurich, Switzerland, pp.1699-1707.

Rogova, E., Lodewijks, G., Pang, Y. (2014) Application of standards in reliability prognosis of braking system of moving walks. Proc. *European Safety and Reliability conference (ESREL)*, Wroclaw, Poland, pp.1289–1297.

Santos, F.P., Teixeira, A.P., Guedes Soares, C. (2014) An age-based preventive maintenance for offshore wind turbines. Proc. *European Safety and Reliability conference (ESREL)*, Wroclaw, Poland, pp.1147-1155.

Sharma, V.K, Agarwal, M., Sen, K. (2011) Reliability evaluation and optimal design in heterogeneous multi-state series-parallel systems. *Information Sciences*, 181, pp.362–378.

Sun, L. and Jia, Y. (2011) Research of equipment reliability prognosis model based on SVR. *2011 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE); Proc. intern. conf., Xi'an, China, 17-19 June 2011*. IEEE.

The Institute of Electrical and Electronics Engineers, Inc. (1985) *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems.*

Wang, Y. and Li, L. (2012) ‘Heterogeneous Redundancy Allocation for Series-Parallel Multi-State Systems Using Hybrid Particle Swarm Optimization and Local Search’. *IEEE Transactions On Systems, Man, And Cybernetics—Part A: Systems And Humans*, 42(2), pp.464-474.

Zio, E. (2013) *The Monte Carlo Simulation Method for System Reliability and Risk Analysis*. Springer Series in Reliability Engineering.

Chapter 3

Functional safety in braking system redundancy requirements for moving walks*

As was shown in Chapters 1-2, reliability of the braking system of moving walks plays a major role in the safe exploitation of these people movers. According to the requirements of the standard ISO 22201-2, described in Chapter 2, the reliability of a braking system of a moving walk has to correspond to safety integrity levels in a range from SIL1 till SIL3. In order to satisfy the required safety integrity level, a reliability analysis of a braking system will be performed in this chapter using a probabilistic method and the Weibull distribution model. This Chapter will present the results of the reliability analysis and show the necessity of redundancy of the braking system of public service moving walks. The results for the proposed redundant design show a higher reliability level than compared to braking system designs without redundancy. Based on these results and using probabilistic and diagnostics approach, a suggestion for an intelligent system for preventing failure in a braking system is presented in this Chapter.

The rest of this Chapter is organized as follows. Section 3.2 describes a method for determination of safety integrity requirements and a reliability analysis of a braking system of moving walks. Section 3.3 contains proposals for enhancement of reliability such as redundancy architecture and a diagnostic system. Section 3.4 presents general results, a comparison of obtained graphs of PFH (average frequency of dangerous failures) before and after applying redundancy, and introduces an intelligent system for SIL maintaining. Section 3.5 presents a proposal for application of functional safety concept to the design of belt conveyors and identifies main issues. Section 3.6 lists the conclusions.

* This chapter is a revised version of two papers: E. Rogova, G. Lodewijks (2015); G. Lodewijks, E. Rogova (2014).

3.1 Importance of brakes in passenger conveyors

Moving walks and escalators are passenger conveyors. They are for example used in airports, grocery stores, transport terminals, fair grounds and railway stations. These conveyors carry many people in public places every day. Therefore, the operational safety of these conveyors is very important. Although moving walks and escalators have safety precautions, they still have accidents in practice. Some of these have tragic consequences, including casualties. Many tragic accidents happen because some people, that use the conveyor, fall. According to Consumer Product Safety Commission (CPSC) data, 16 people were killed on escalators in the period 1997 till 2006 in the USA caused by a fall on an escalator (Mccann and Zaleski, 2006). CPSC estimated that this is about 75% of all accidents for this period of time. About 2.5% of all escalator stops lead to passenger falling (Al-Sharif, 2006).

As was mentioned in Chapter 1, The Washington Post described an escalator accident in which six passengers were injured. An “overspeed fault”, which shut down the escalator’ motors, automatically engaged the brakes. Officials said that all three brakes engaged but that they failed to slow down the escalator. The first brake because it was covered in oil, the second brake because it “showed wear” and the third brake even though it was in “good condition” (Scott Tyson, 2010). This example demonstrates, that it is not enough to just apply redundant brakes without diagnostic system, even in case of three brakes. The most important aspect is to conduct appropriate maintenance, to plan inspections and to replace/repair components in time. This replacement/reparation should be based on data obtained from a diagnostic system and on a prognosis of the equipment condition. The construction of escalators and moving walks is very similar which allows comparison of accidents. In case of all kinds of accidents (falls, caught in/between) the conveyor has to be stopped within an acceptable braking distance to avoid injury (Al-Sharif, 2006). This implies that a brake system in all cases acts as the actuator of the safety system for injury preventing.

The standard EN 115-1, safety of escalators and moving walks, recommends equipping these conveyors with two types of brakes: an operational brake and an auxiliary brake (EN 115-1, 2010). The installation of auxiliary brakes is required only for inclined moving walks under special conditions. Auxiliary brakes, also called emergency brakes, shall be of the mechanical type. The most widely used types of brakes for operational braking are hydraulic and electromagnetic brakes (Al-Sharif, 2006). Hydraulic brakes allow proportional control easier than electromagnetic brakes. Their brake torque can be controlled proportionally by changing the oil pressure (Al-Sharif, 2006). This allows intelligent braking where the brake torque can be adjusted in accordance to the requirements. Intelligent braking is better than conventional braking because the maximum deceleration rate of the conveyor can be controlled. However, it is impossible to design an intelligent system that is 100% reliable (Al-Sharif, 2006). But it is possible to estimate risks and to improve the reliability of an intelligent braking system.

These days more and more solutions for intelligent braking systems appear. Patents of the CONE corporation and the ThyssenKrupp elevator innovation center made a contribution for the improvement of a braking system for passenger conveyors. CONE presented a method for regulating the brakes independently of the load (Balzer-Apke et al., 2003). ThyssenKrupp suggested solutions of constant braking distance regardless of the load (Gonzalez Alemany et al., 2013), which requires a proportional brake. There are no doubts that the overall reliability of moving walks increases because of an improvement of the braking system. However, what kind of improvements should be done to increase the reliability and are they necessary or not?

Reliability improvement can be achieved in several ways. The first way is by adding redundancy to a system. The second way is by using diagnostics. The third way is a combination of the first and the second way. Unfortunately, often specialists that consider safety questions of passenger conveyors suggest redundancy as a reliability improvement measure, without justification of why the conveyor needs it and whether it is sufficient. Indeed, at the design stage of projects, “the redundancy allocation is a direct way of enhancing reliability” (Tavakkoli-Moghaddam et al., 2008). The decision to apply redundancy for a braking system however is very complex. It is a question of additional equipment, changing design and requiring extra funding. Sometimes redundancy is excessive, sometimes it is necessary. The choice depends on a few parameters such as safety requirements for the conveyor, rate of reliability degradation and the conditions of exploitation.

European standard EN 115-1 defines operating conditions of moving walks for public transport. Moving walks should be “suitable for intensive use, regularly operating for approximately 140 h/week with a load reaching 100% of the brake load for a total duration of at least 0,5 h during any time interval of 3 h" (EN 115-1, 2010). "The load conditions and additional safety features should be agreed between the manufacturer and the owner reflecting the traffic levels which exist…" (EN 115-1, 2010). Operating conditions depend on the duration of work per day, the people flow, the existence of a "spare" moving walk to replace a broken machine at any time. If people flow is small or if there is a second moving walk for people transportation during repairing of the first one, redundancy is not necessary. It is enough to provide a machine with a diagnostic system in this case. If the people flow is quiet large and if there is no "spare" moving walk, a redundant system with diagnostics of failures is necessary. For example, the machine has to be in operation 24 hours per day, 7 days per week like moving walks in Los Angeles World Airports (Los Angeles World Airports, 2011). The question of reliability of a braking system for moving walks with such operating conditions and the lack of a spare moving walk is one of the most important. The operational condition of 24/7 is hard. Repair of a moving walk in that case is possible only at the limited period of time. This is especially actual for airports and big malls. Therefore, the focus is on an operational braking system with a hydraulic type of brakes for public service moving walks with lack of a spare moving walk and operating conditions "24/7".

The aim of this Chapter is to estimate safety integrity requirements for a braking system of moving walks, to conduct a reliability analysis of a braking system in accordance to International and European standards, and to define necessity of redundancy of a braking system. The results obtained in this Chapter confirm the necessity of a redundant braking system for moving walks with described operating conditions. Introduced intelligent system with two maintenance mode (economical and full) is able to maintain the required safety integrity level (SIL), not only for the braking system, but also for other technical systems with degradation of their reliability parameters over time. This study also will identify the lack of analytical formulas of reliability assessment for systems with non-constant failure rates in safety standards.

3.2 Reliability of a braking system

This section outlines the method of probabilistic (reliability analysis) approach of failure prediction based on requirements of safety standards. Calculations presented in this section, illustrate common method for defining the necessity of redundancy of a braking system. The calculations are for illustration purposes only and cannot be considered as direct calculations for any type of braking system.

3.2.1 Elements of risk analysis: determination of SIL requirements

As a guideline for the analysis of the safety integrity level of a braking system of moving walks, the standards IEC 61508 and ISO 22201-2 have been chosen. The method described in the IEC 61508, consists of two stages: determination of the safety integrity level (SIL) requirements for the system (or the general integrity constraints for the braking system), and the estimation of the SIL by reliability analysis for equipment of the system in accordance to SIL requirements (IEC 61508-1, 2010). Determination of SIL requirements is needed if the data about SIL for the selected safety function are absent. In this case SIL has to be determined based on risk analysis.

The safety integrity level (SIL) is defined by the standard IEC 61511-1 as "a discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems" (IEC 61511-1, 2004). The highest and most reliable level is SIL4, the lowest level SIL1. As was mentioned earlier in this Chapter, there are limitations for specifying SIL for escalators and moving walks, defined by ISO 22201-2. Safety-related function shall be no less than SIL 1 and no greater than SIL 3. SIL 4 is not allowed for escalators and moving walks "as it is not relevant to the risk reduction requirements normally associated with machinery" (IEC 62061, 2005).

A functional safety model considers safety functions and safety systems that perform the safety functions. Safety functions have a SIL that can be determined. The SIL of a safety system has to correspond to SIL of a safety function. If the SIL of a safety system is less than the corresponding SIL of a safety function, the system needs to be improved. Improvements can be made by adding redundant systems, by changing the design of the system or replacing components, by changing the architecture of safety systems, and by changing the applied maintenance strategy.

For the determination of SIL requirements an ALARP (‘As Low As Reasonably Practicable’) model and tolerable risk concepts recommended by IEC 61508-5 and ISO 22201-2, are used here. To receive the value of SIL, this method allows to qualify risk (intolerable, undesirable, tolerable, negligible) and to define the class of risk quantitatively. An ALARP model is good for both a qualitative and a quantitative risk estimation (IEC 61511-3, 2004). To make a conclusion about the necessity of redundancy of a braking system, a quantitative risk estimation has to be implemented. It is important to mention that SIL should be defined for safety functions (IEC 61511-1, 2004). There are many safety functions in moving walks. But with respect to the braking system there is a final safety function “Stop machine”, which can be the result of work of other safety functions. Determination of SIL is conducted here for this final safety function.

In accordance to the ALARP-model (IEC 61508-5, 2010), four consequence levels of moving walks accidents are defined: catastrophic (Ca), major (Ma), severe (Se) and minor (Mi). Table 3.1 demonstrates correspondence between the duration of machine unavailability and the consequences of an accident in relation to the amount of injuries/deaths. This table is an interpretation of the Table “Quantitative consequence categories” in the manual for APCS engineers “Risk analysis of technological system in Interlock system conception for ITER” (Rogova, 2012). The table is adapted for people transportation equipment, and considers number of sacrifices instead of money cost like in the table developed for ITER. Table 3.1 can have some changes in categorization of accident consequences and duration of brakes unavailability: it is not a general rule which is common for all passenger conveyors.

Six frequency categories are defined in IEC 61508 and ISO 22201-2. Table 3.2 shows correspondence between the name of the category and the probability of the occurrence of an accident.

Table 3.3 demonstrates how to define a risk class in accordance to ISO 22201-2. Obtained from Table 3.3 risk classes (ISO 22201-2, 2013) can be transformed to safety integrity levels in accordance to IEC 61508-6.

Table 3.1: Determination of severity of accident consequences.

	Brakes Unavailability				
Consequences of an accident	**<1 hour**	**< 1 day**	**<2 days**	**<1 week**	**<1 month**
< No injuries	Mi	Se	Se	Se	Se
No significant injuries	Se	Se	Se	Ma	Ma
<5 severe injuries	Ma	Ma	Ma	Ma	Ca
< 10 and >5 severe injuries	Ma	Ma	Ma	Ca	Ca
>=1 death and/or multiple severe injuries	Ca	Ca	Ca	Ca	Ca

Table 3.2: Occurrence probability in events per year (ISO 22201-2, 2013).

Category	Potential frequency for effect	Mean value per year per unit moving walk	Mean value for total (2000) population per year
Frequent	≥0,01	0,01	20
Probable	0,001 – 0,01	0,005	10
Occasional	0,0001 – 0,001	0,0005	1
Remote	0,00001 – 0,0001	0,00005	0,1
Improbable	0,000001 – 0,00001	0,000005	0,01
Negligible	< 0,000001	$4{,}16667 \times 10^{-7}$	0,000833

Table 3.3: Determination of risk class (ISO 22201-2, 2013).

	Accident consequences			
Event probability	**Catastrophic**	**Major**	**Severe**	**Minor**
Frequent	IA	IIA	IIIA	IVA
Probable	IB	IIB	IIIB	IVB
Occasional	IC	IIC	IIIC	IVC
Remote	ID	IID	IIID	IVD
Improbable	IE	IIE	IIIE	IVE
Negligible	IF	IIF	IIIF	IVF

To demonstrate how to use the described method, concrete values of machine unavailability, accident consequences and occurrence probability in events were chosen. For estimation it was assumed that an average machine unavailability is *less than 1 day*. The most frequent accident consequences are *No significant injuries.* Intersection of the column and the row of Table 3.2 gives consequence level *Severe*. If the number of accidents is about *1 per year,* this allows to define the category of occurrence probability: *Occasional* (Table 3.2). Intersection of the column *Severe* and the row *Occasional* of Table 3.3 gives the risk class *IIIC*.

Unfortunately, the standard ISO 22201-2 does not provide readers with the table of correspondence between risk classes and SIL. Such table of correspondence between risk classes and SIL could serve a very useful and practical tool. However for the moment it is a topic of future research. The SIL assignment matrix obtained as an intersection of severity level and class of probability of harm (Cl), is provided by IEC 62061 (IEC 62061, 2005) and can be used as a basis for development of table of correspondence between risk classes and SIL.

Determination of a safety integrity level is conducted here by means of risk graph method, described in IEC 61508-5. Comparing to a quantitative method, a risk graph method considers more possible situations that allow to estimate SIL more accurate. The method determined that risk class *IIIC* corresponds *SIL2* for this system. The obtained value of SIL=*SIL2* is appropriate for the requirements of the standards ISO 22201-2 and EN 115-1.

Described method of the determination of general integrity constraints for the braking system can be used for all subsystems of moving walks. The biggest challenge of using of this method is the accuracy of determination of SIL requirements. Correct determination of SIL requirements means correct equipment selection in accordance to SIL requirements. Loss of accuracy can happen due to wrong data of accident consequences, duration of machine unavailability and method of transforming of risk class to SIL.

3.2.2 Reliability assessment of a braking system

The braking system of a moving walk consists of electro-mechanical, hydraulic and electronic equipment. The system was classified as a type A subsystem according to IEC 61508-2 since failure modes of all constituent components are well defined. For an approximate reliability assessment of a braking system the following configuration was chosen: a hydraulic disk brake, brake pads, the required hydraulic power unit and brake controller.

The main representation of the system was obtained through a Reliability Block Diagram (RBD) – one of the methods recommended by IEC 61508. RBD was chosen due to the block structure of a braking system. There are different components: mechanical and hydraulic components with strong degradation of parameters and a reliable controller. Therefore, the best way to consider the reliability of an overall system with different components is a *block way*: the braking system, divided into simplified blocks (components), is demonstrated in Figure 3.1. Each block has its own data in terms of reliability (IEC 61078, 2006). The block of Main Controller was also included to the RBD of the braking system, because control signals go from the Main Controller to the Brake Controller, and it takes part in the reliability calculations.

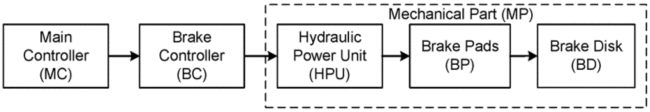


Figure 3.1: RBD of the braking system (BS).

The braking system is considered as a high demand system since an interlock event of the BS is supposed to happen more often than once a year. A braking system is considered as executing in a continuous mode. Therefore, the analysis was focused on calculation of average frequency of dangerous failure (PFH) for different components.

The general equation for the calculation of the PFHs for a system consisting of serial blocks of RBD is (IEC 61508-6, 2013):

$$PFH_S \approx \sum_{i=1}^{N} PFH_i \qquad (3.1)$$

Equation 3.2 describes the reliability of the braking system being the sum of the reliability of the individual components:

$$PFH_{BS}(\tau) = PFH_{MC} + PFH_{BC} + PFH_{MP}(\tau) \qquad (3.2)$$

where τ is a test interval.

The main and brake controllers are electronic devices. Failure rates of these devices are approximately constant. For an estimation of the reliability of the MC block the controller Siemens SIMATIC S7-300 was chosen. This controller is used in order to meet all requirements in terms of safety and fault-tolerance. The configuration of this controller and the PFH of its modules are shown in Table 3.5. The configuration of the brake and the main controller (BC and MC blocks) was chosen based on the controller Siemens S7-300.

To estimate the reliability of a braking system, it is necessary to obtain the PFH of the system. Taking into account the degradation of the parameters in the mechanical part MP, it was decided to apply a distribution of probabilities of failure and to calculate the overall PFH value of the braking system at several periods of time.

Table 3.5: PFH values for Main and Brake Controller components.

Module	PFH
CPU 315-2 PN/DP	1.00E-08
IM Interface (CPU to I/O) IM 151-8 PN/DP CPU	2.00E-08
Profinet	5.00E-09
SM-326 Digital Output Card	1.00E-08
SM-326 Digital Input Card	1.00E-08
SUM:	5.5E-08

For the reliability analysis of the mechanical part (MP block on RBD diagram) with non-constant failure rates, different types of mathematical distributions were considered. For instance, the log-normal distribution is widely used in scientific fields such as agricultural, entomological, biological etc. The obtained values of this distribution however are “difficult to interpret and use for mental calculations” (Limpert et al., 2001). Even so, although “there are many statistical distributions other than the Weibull, the log-normal distribution is the second choice for life data analysis” (IEC 61649, 2008). The standard IEC 61810 states that “as the failure rate for elementary relays cannot be considered as constant, particularly due to wear-out mechanisms, the times to failure of tested items typically show a Weibull distribution” (IEC 61810-2, 2011). For this research it was necessary to find a distribution that takes into account the degradation parameters of the different mechanical components and that is suitable for a reliability calculation of the braking system. Thereby, on the basis of recommendations of standards and literature review, Weibull distribution was chosen as a distribution of failures of degrading components.

Firstly, a Weibull analysis has a few main advantages such as reasonably accurate failure analysis, a failure forecast with a very small samples, and a simple and useful graphical plot of the failure data (Albernethy, 2004). Secondly, there are data bases with Weibull shape factors α and characteristic life η parameters for all main types of mechanical equipment that makes engineering calculations of reliability with Weibull very suitable. This distribution allows obtaining the failure rate function as an equation depend on time t, α and η (see Equation 2.1, Chapter 2). Weibull parameters of hydraulic braking system are required for calculation of reliability by using the considered here approach. If this information is not available, the most critical components and failure modes should be considered. Mechanical part of braking system consists of: hydraulic cylinder, DC motor, solenoid valve, pump, check valve, relief valve, springs, braking disk and pads. It is also possible to consider similar braking systems with known Weibull parameters.

Final values of the PFH$_{BS}$ of braking system were obtained in accordance to Equation 3.2 for seven periods of time: 1 month, 6 months, 1 year, 2 years, 3 years, 4 years and 5 years. Values of Weibull parameters that are used here for calculation of mechanical part are obtained for hydraulic braking system of wind turbines: α=1.7459; η= 82942 (Selwyn, 2012). Until now there is no research about estimation of Weibull parameters for a braking system of moving walks. Therefore Weibull parameters can be different for braking systems of moving walks and wind turbines. However in case of availability of required parameters for moving walks, the calculations can be easily repeated. PFH values of a braking system and a system entirely together with controller part (main and brake controller) for 7 periods of time are given in Table 3.6.

Table 3.6: PFH$_{MP}$ values of mechanical part and BS entirely without redundancy.

PFH	$PFH(0,\tau)$	$PFH(\tau,2\tau)$	$PFH(2\tau,3\tau)$	$PFH(3\tau,4\tau)$
	0-6 month	**6months -1 year**	**1-1.5 years**	**1.5-2 years**
MP	$1.3443\cdot10^{-6}$	$3.1645\cdot10^{-6}$	$4.6428\cdot10^{-6}$	$5.9710\cdot10^{-6}$
System entirely	$1.3993\cdot10^{-6}$	$3.2195\cdot10^{-6}$	$4.6978\cdot10^{-6}$	$6.0260\cdot10^{-6}$
PFH	$PFH(4\tau,5\tau)$	$PFH(5\tau,6\tau)$	$PFH(6\tau,7\tau)$	$PFH(7\tau,8\tau)$
	2-2.5 years	**2.5-3 years**	**3-3.5 years**	**3.5-4 years**
MP	$7.\ 2039\cdot10^{-6}$	$8.3682\cdot10^{-6}$	$9.4793\cdot10^{-6}$	$1.0548\cdot10^{-5}$
System entirely	$7.\ 2589\cdot10^{-6}$	$8.4232\cdot10^{-6}$	$9.5343\cdot10^{-6}$	$1.1098\cdot10^{-5}$

The obtained results demonstrate strong degradation in terms of reliability from SIL2 till no SIL. Table 3.7 shows correspondence between SIL and the PFH values:

Table 3.7: Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation (IEC 61508-1, 2010).

SIL	Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

The SIL estimated by a reliability analysis of the braking system has to correspond to SIL requirements (SIL2) as defined by ALARP in Section 3.2.1. However, the Tables 3.6 and 3.7 show that braking system mainly corresponds to SIL1 for the considered time intervals that is not appropriate for SIL requirements defined as SIL2. The system requires some arrangements to improve reliability.

3.3 Enhancement of reliability of a braking system

3.3.1 Redundancy architecture

As was described before, the scope is on public service moving walks with operating conditions “24/7”. The method, suggested in this section, defines a scope of future works for repairing and maintenance of a braking system, estimates the period of time for execution of this work and reports about fault in advance before failure will come. A redundant system with diagnostics allows planning repair of the main braking system at a convenient time.

Two ways of prediction of failure should be considered: probability approach, described in Section 3.2, and “diagnostic + redundancy” approach. The probability approach predicts economical costs for repair in the future (amount of equipment that should be replaced in future and approximately when). The “diagnostic + redundancy” approach gives more exact time of repair and allows to significantly reduce the amount of dangerous failures.

Combination of these two approaches gives an increase of reliability and convenient maintenance, based on prediction.

As was described in Section 3.1, even three installed brakes can fail in case of a lack of appropriate diagnostics of the equipment. In this research it will be shown that two brakes (one of them is redundant) with diagnostics of the braking system of moving walks are enough to keep an appropriate SIL.

As a redundancy architecture for a braking system, the voting logics M-out-of-N was chosen. F system is an N-component system which fails when any M of its N components fail (Kuo et al., 2001). M-out-of-N architecture was chosen because this architecture is the most general form of redundancy, recommended by IEC 61508. Other types of redundancy, such as parallel passive, parallel active, majority voting redundancy, are special cases of M-out-of-N redundancy architecture.

The 1oo2D architecture was chosen for redundancy of braking system. This architecture is a partial case of M-out-of-N (MooN) systems. It means that in case of a fault signal from any of two sensors, the system will be switched to redundant. Signals from two incremental sensors, which are a part of a diagnostic system (Section 3.3.1) go to the MC for processing. Architecture 1oo2D combines stability of 1oo2 architecture with respect to dangerous failures, stability of 2oo2 architecture with respect to spurious trips, and detailed self-test and mutual channel diagnostics. In systems with 1oo2D architecture four channels work parallel: two main and two diagnostic. This can help to achieve the highest safety level and fault tolerance (Fedorov, 2008). A physical block diagram of the 1oo2D architecture is shown in Figure 3.2.

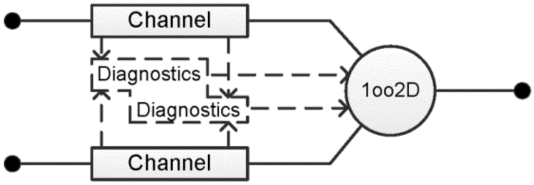


Figure 3.2: 1oo2D physical block diagram (IEC 61508) (IEC 61508-6, 2013).

A diagnostic system of 1oo2D architecture of a braking system of moving walks consists of an incremental sensor (encoder) and uses a main controller for the calculations of the diagnostic function. The PFH value of the incremental sensor is appropriate for SIL3: $PFH_{Incr.Sens}$=1,09 x 10^{-8} h^{-1} (Kubler Group, 2013).

The functional scheme of the diagnostics for a braking system with 1oo2D architecture is shown in Figure 3.3. This scheme was developed based on the requirements of the standard IEC 61508-6 for 1oo2D architecture, and applied to the braking system of moving walks.

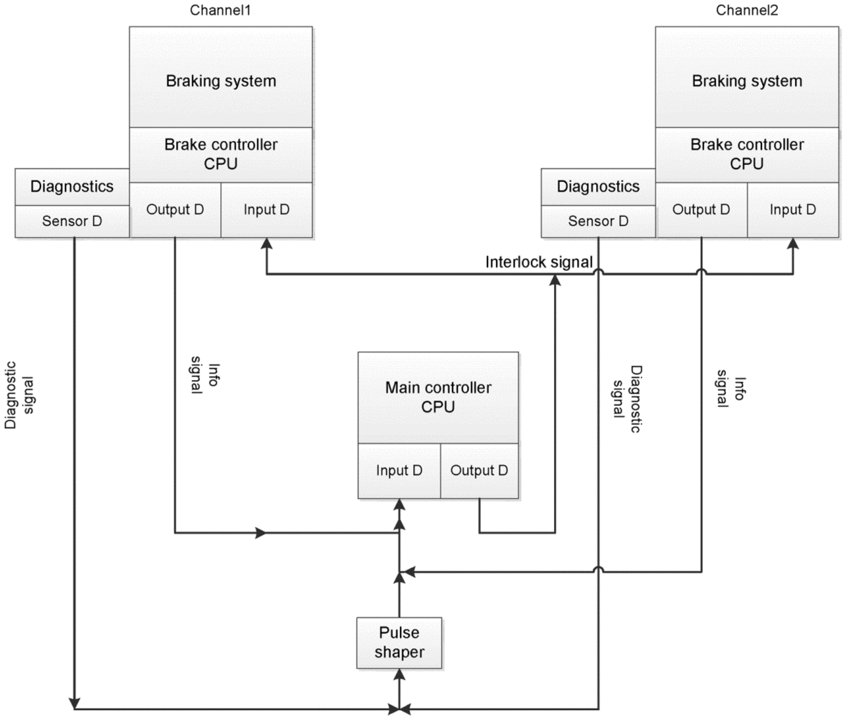


Figure 3.3: Functional scheme of diagnostics for a braking system.

Figure 3.3 demonstrates the 1oo2D architecture for a braking system. Two identical braking systems have a ‘brake controller’, which consists of CPU, digital input and digital output. The logics of the 1oo2D architecture is processed in the CPU of the Main Controller of a moving walk. The interlock signal, produced by the CPU, means command “stop machine” and goes from the digital output of main controller to the digital input of brake controller. The diagnostic signals go from the digital incremental sensors via the Pulse shaper to the digital input of the Main controller for further processing. The pulse shaper is required to transform the sine/cosine output of the sensor to rectangular pulses. Reasons for choosing this sensor are given in Section 3.3.2.

There are also info signals from brake controller. These are only information signals about all stop cases and other additional information, which is necessary for the statistics and for the operator.

Diagnostics is an ‘indicator’ to switch to a redundant system. It is an integral part of the 1oo2D architecture. Diagnostics indicates a fault of the braking system and sends the signal “switch to redundant system”.

3.3.2 Diagnostics of braking system

As was mentioned in the previous section, a diagnostic system is a part of the 1oo2D architecture. The working principle of this diagnostic system is based on the duration of pulses from an incremental sensor (encoder). After the main controller sends the signal “STOP” to the brake controller, the braking disc starts to slow down. If the pulse duration, obtained from the incremental sensor, is less than it should be, braking is not performed effectively (i.e. disc rotates faster than it is needed during the braking process). The choice of the sensor for this diagnostics depends on a few parameters: reliability and the number of pulses per revolution. To define the required number of pulses for the sensor, the allowable angular displacement of the walking surface at rest condition was calculated. The incremental sensor is located on the shaft of drive pulley. Based on this, angular displacement was calculated in accordance to Equation 3.3:

$$\theta = \frac{360l}{\pi d} \tag{3.3}$$

where l - a value of allowable displacement of walking surface at rest condition; d - a diameter of pulley of moving walk.

The allowable longitude displacement of a walking surface l is 4 mm in accordance to requirements of EN 115-1 (EN 115-1 2010); a value 0,5 m was chosen as a diameter d of the pulley of a moving walk for the estimation of the angular displacement (Figure 3.4). According to these data and Equation 3.3, the angular displacement θ is equal $\approx 1°$. Thus, the minimum number of pulses N_θ corresponds to the amount of pulses per θ and characterizes the rest condition. For an estimation of the N_θ , error of measurement of number of pulses was chosen as ±1 pulse. The number of pulses with a margin is equal to 4 pulses. It means that at rest condition the sensor issues 4 pulses. In case of a slow movement the number of pulses will be more than 4 pulses, which helps to differ the rest condition from the slow movement of the moving walk. The estimation of the maximum number of pulses N_{max} was obtained in accordance to Equation 3.4 and is equal to 1440 pulses per revolution (Table 3.8).

$$N_{max} = 360° * N_{\theta} \tag{3.4}$$

As an incremental sensor, the Sendix 5814 FS3 sensor was chosen. The sensor meets two main requirements: high reliability and the required number of pulses. The reliability of this sensor is appropriate for SIL3 and maximum number of pulses is 2048 per revolution. The incremental information of the Sendix 5814 FS3 is provided by an analogue sine/cosine signal (Kubler Group, 2013). The pulse shaper, installed before the main controller, transforms sine to rectangular pulses and gives the picture shown in Figure 3.5.

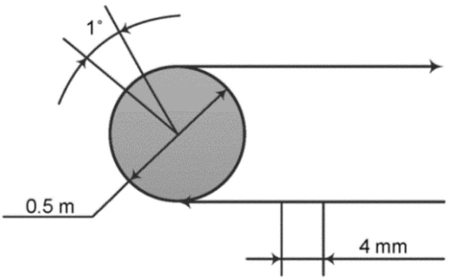


Figure 3.4: Displacement of walking surface at rest condition.

Table 3.8: Number of pulses

Degree (θ°)	Pulses
1	4
360	1440

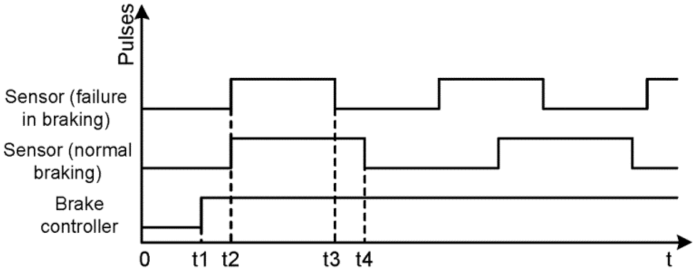


Figure 3.5: Diagram of pulses for a diagnostic system.

The duration of the pulse is proportional to the rotational speed. In Figure 3.5 t1 is the beginning of pulse from Brake controller when it issues the signal “STOP MACHINE”. The time t2 is the beginning of the pulse from the

Incremental sensor. The time difference (t2-t1) is the period of time, in which it is necessary to control the efficiency of braking. Time t2 can be estimated by an experimental method, for example, for the worst case (the most loaded case) or by a special control function. The mass and the inertia of moving walk depends on loading (amount of passengers). Thus, the time t2 depends on the moving walk loading. Moving walks with different loading has to brake differently.

The special control function recalculates permanently the value of time t2 for different loadings in real time. This function depends on the motor current. The more current - the greater the loading. Thus, it is possible to derive a dependence between current and loading: the greater loading – the later control pulse duration (starting from t2) will be started.

The time difference (t3-t2) is the duration of a short pulse: if the disc rotates faster than it should be in case of a normal operation then that means a fault. The main controller generates the signal “To SWITCH” the main braking system to the redundant braking system. The time difference (t4- t2) is a duration of normal pulse: the braking system works normal. If a pulse duration is more than it is allowed, then the fault signal during the braking is issued and it switches to the redundant braking system. The redundant braking system must run periodically as a main to test its performance.

3.3.3 Calculation of redundant braking system

The block diagram of the redundancy architecture presented in the functional scheme of diagnostics for a braking system (Figure 3.3) is shown below. In one channel there is not only mechanical part with non-constant failure rate modeled by Weibull distribution, but also two constant failure rates related to a brake controller and an incremental sensor for a diagnostics:

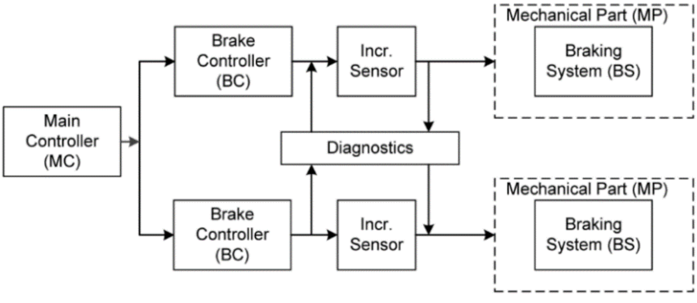


Figure 3.6: Block diagram of 1oo2D redundancy architecture for a braking system.

The analysis of safety standards conducted in Chapter 2, showed the lack of analytical formulas which can be applied for PFH calculation of M-out-of-N redundancy architecture with non-constant failure rates. Formulas proposed by IEC 61508, can be applied only for systems with constant failure rates. Therefore here for calculation of PFH value of 1oo2D architecture, the new formula is proposed (Equation 3.5). The details of derivation of PFH formula for general M-out-of-N redundancy architecture with non-constant failure rates can be found in Chapter 4.

$$\begin{cases} PFH^{RBS}\big((i-1)\tau, i\tau\big) = \binom{N}{N-M+1} \cdot \left(\frac{(1-\beta)z_D(\tau)}{\alpha}\right)^{(N-M+1)} \cdot \tau^{N-M} \cdot \\ \cdot \left(i^{\alpha\cdot(N-M+1)} - (i-1)^{\alpha\cdot(N-M+1)}\right) + \frac{\beta\cdot z_D(\tau)\cdot(i^{\alpha}-(i-1)^{\alpha})}{\alpha}, \\ PFH^{SYS}\big((i-1)\tau, i\tau\big) = PFH^{RBS}\big((i-1)\tau, i\tau\big) + PFH_{MC}; \end{cases} \tag{3.5}$$

where β=0.02– common cause failure factor; N=2, M=1; DC (diagnostic coverage) = 0.9; τ=6 months; α – Weibull shape parameter (for a channel)

As shown in Equation 3.5, obtaining the PFH^{RBS} value of a braking system with applied redundancy architecture, requires the failure rate function of one channel. However the failure rate function of one channel demonstrated in Figure 3.6, consists of the failure rate function of mechanical part MP, and constant failure rates of brake controller BC and incremental sensor. In this case the distribution of failures of a channel is not Weibull anymore, and Equation 3.5 cannot be applied. However, constant values of PFH of a brake controller and an incremental sensor can be neglected in case of a minor contribution to the value of a failure rate function for the considered period of time (5 years).Two failure rate functions for a braking system with account of constant part (brake controller and incremental sensor) and without them are presented in Figure 3.7. This figure shows that the difference between these two functions is very small. Therefore in this study the failure rate contribution from a brake controller and incremental sensor is neglected in calculations of redundant architecture.

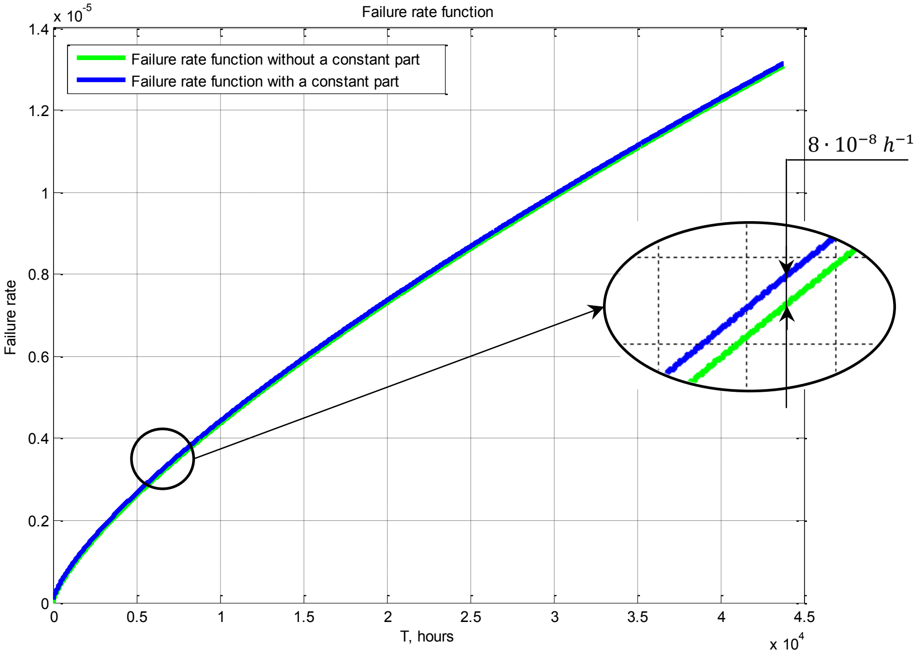


Figure 3.7: Failure rate function of a braking system.

Figure 3.7 demonstrates that after ~1 year the difference between two failure rates is around $8 \cdot 10^{-8}\ h^{-1}$ that is small comparing to the values of failure rates. Certainly, this difference can worsen the PFH values obtained after applying redundancy. A lack of possibility to include several components with constant and non-constant failure rates in one channel is a drawback of the proposed formula (Equation 3.5). However, such simplification can be used for one-component redundancy model or if other contributions to the main failure rate function can be neglected.

Values of the PFH_{RBS} for the braking system with redundancy were obtained for seven periods of time: from 6 months till 4 years and demonstrated in Table 3.9. The obtained values show significant enhancement of reliability after applying redundancy with diagnostic system.

Table 3.9: $\mathrm{PFH}_{\mathrm{RBS}}$ values for braking system with redundancy.

PFH	$PFH(0,\tau)$	$PFH(\tau,2\tau)$	$PFH(2\tau,3\tau)$	$PFH(3\tau,4\tau)$
	0-6 month	**6months-1 year**	**1-1.5 years**	**1.5-2 years**
RBS	$2.7646\cdot10^{-9}$	$7.1081\cdot10^{-9}$	$1.1953\cdot10^{-8}$	$1.8039\cdot10^{-8}$
System entirely	$5.7765e\text{-}\cdot10^{-8}$	$6.2108\cdot10^{-8}$	$6.6953\cdot10^{-8}$	$7.3039\cdot10^{-8}$
PFH	$PFH(4\tau,5\tau)$	$PFH(5\tau,6\tau)$	$PFH(6\tau,7\tau)$	$PFH(7\tau,8\tau)$
	2-2.5 years	**2.5-3 years**	**3-3.5 years**	**3.5-4 years**
RBS	$2.5756\cdot10^{-8}$	$3.5400\cdot10^{-8}$	$4.7218\cdot10^{-8}$	$6.1425\cdot10^{-8}$
System entirely	$8.0756\cdot10^{-8}$	$9.0400\cdot10^{-8}$	$1.0222\cdot10^{-7}$	$1.1643\cdot10^{-7}$

3.4 Results

Based on the obtained results for a monosystem (Table 3.6) and for a system with redundancy (Table 3.9) a reliability graph was built. Figure 3.8 shows a trend for a braking system without redundancy. Figure 3.9 shows a trend for a system after applying redundancy. Comparing these two trends, it can be concluded that redundancy improves the reliability of a braking system. The braking system with applied redundancy architecture 1oo2D meets the requirements of SIL2 obtained in Section 3.2.1. Moreover, the calculated values of PFH show correspondence to SIL3.

The reliability of the system with redundancy is also decreasing. Nevertheless the rate of reliability decrease is much less, than for a system without applying redundancy architecture and diagnostics.

Both the diagnostic approach and the reliability prognosis approach predict possible failures. Diagnostics prevents failure by switching to a redundant system and helps to plan money expenditure for repair of faulty equipment. The SIL-based reliability prognosis gives an approximate time of replacement/repair of equipment. A special intelligent system combines both of these approaches and maintains a safety integrity level required for the braking system. Components of the braking system should be repaired/replaced as soon as an intelligent system will detect that reliability is closing to the border between SILs.

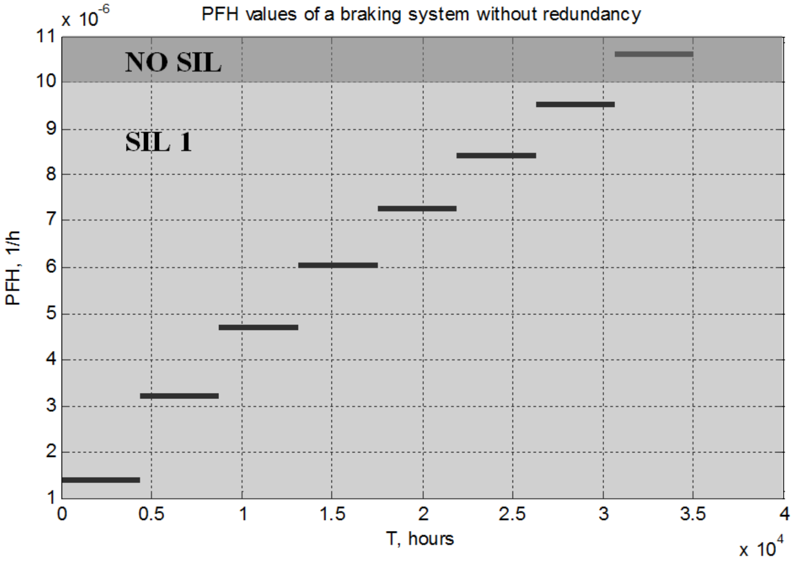


Figure 3.8: PFH values of a braking system (entirely) before applying redundancy.

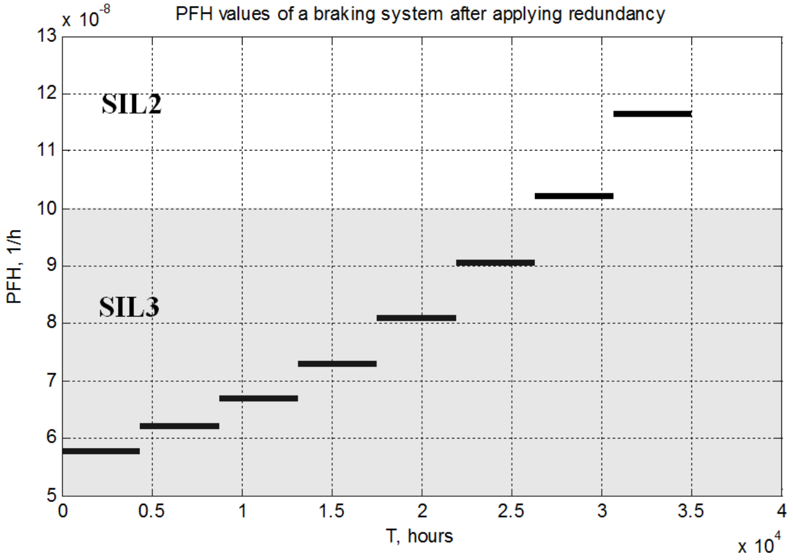


Figure 3.9: PFH values of a braking system (entirely) after applying redundancy.

SIL prognosis in Figure 3.8 demonstrates that the system does not correspond to SIL2. In case of a braking system after applying redundancy and diagnostics (Figure 3.9) SIL prognosis shows correspondence to SIL 3 for more than 3 years. The idea of SIL-prognosis is estimation of time when calculated reliability is approaching the "border" between "SIL-zones". This should be considered as a time of periodic repair/maintenance (t_{per}). Such intelligent system keeps track of the safety level of a braking system by means of diagnostic and reliability prognosis approaches.

If an intelligent system detects that the reliability of a braking system is close to the border between SILs, the operator will see an alarm signal on the monitor. It is suggested to add a special "Reliability trend" in addition to other trends of SCADA for monitoring of buildings that have transport systems. An intelligent system informs an operator in advance about the necessity to repair/replace an element of a braking system before the system will come through the border between SILs. An intelligent system recalculates the system reliability periodically after each inspection with repairing/replacement of components (see Figure 3.10).

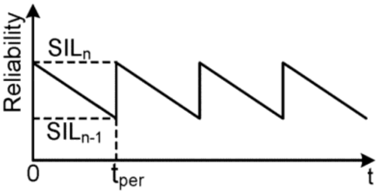


Figure 3.10: Simplified graph of work of an intelligent system in a full mode.

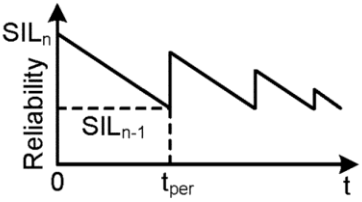


Figure 3.11: Simplified graph of work of an intelligent system in an economical mode.

Maintenance policies using probabilistic and diagnostic approach can be varied depending on economic conditions of a company. After the intelligent system "informs" an operator about the close "border" between SILs, the operator/engineer should take a decision about the appropriate time of maintenance. In most cases after t_{per} (Figure 3.10) some systems can be repaired, in some cases - replaced. Depending on the measure of the parameters degradation for each mechanical component, an intelligent system will recalculate the overall reliability of a system after the replacement and repairing.

The "Economical mode" of repairing in accordance to the corresponding SIL means repair of the most wear-out components. Overall reliability of the system will be increased, but not till the previous level of reliability (Figure

3.11). The “Full mode” (Figure 3.10) can be an expensive option: it means repair of all the wear-out components with full system recovering till the previous level of reliability. Figure 3.11 demonstrates, that the time between periodical repairs of a system is reduced in case of regular partial repair of components in “economical mode” of maintenance. The time t_{per} is constant in a "full mode".

3.5 Application of the functional model to the design of belt conveyors

Described in the previous sections procedure of risk and reliability assessment of a braking system of moving walks in the concept of functional safety is applicable not only to passenger conveyors. It can be and should be applied also to belt conveyors that are not designed for people transportation. Belt conveyors are widely used in the bulk materials handling industry. Since a belt conveyor has many moving components they might form a threat for people working around them if they are not properly shielded. In addition, belt conveyors with high installed power or moving at high speeds store a significant amount of kinetic energy. The high belt tension provides high potential energy. The kinetic and potential energy stored in a belt conveyor can cause catastrophic damage when suddenly released. For example, when a belt breaks, although the belt is not designed to allow this. Some belt conveyors transport people in mines - man riding conveyors. These conveyors can be very dangerous if they do not function as designed.

Despite the fact that there might be safety risks involved in the operation of a belt conveyor, the design standards for bulk material belt conveyors do not address safety issues. A safety integrity level (SIL) defined as a discrete number for specifying the safety integrity requirements of safety functions can be used advantageously at the design stage of belt conveyors. A SIL can assist in making decisions on the redundancy of components, like brakes or brake components; the architecture of safety systems; and the proposed maintenance strategy of belt conveyors.

3.5.1 Four reasons to consider functional safety in belt conveyors

When designing belt conveyors, commonly used for the transportation of bulk solid materials, several design codes are taken into account, like the CEMA (Conveyor Equipment Manufacturers Association) standard or DIN 22101. These standards are primarily focused on determining the friction that the belt will experience during operation. This friction depends on, among other things, the belt conveyor's length, its capacity, the selected belt speed, the belt weight, and the idler roll diameter (Lodewijks, 1995). After the friction is accurately determined, all the major components can be sized including the belt, the drives and the brakes. The standards mentioned therefore provide a typical conventional engineering approach.

Current design standards however, fail to address two important issues. The first issue, for example discussed by Lodewijks (Lodewijks, 2002), is the dynamics of belt conveyors. For large-scale belt conveyor systems, high powered systems or systems with a high capacity, the dynamics during the transient state of the conveyor dictate the design of the conveyor. The second issue that the design standards do not address is safety requirements. Although the design standards specify the safety factors applicable to belt tensions when determining the required belt rating, they do not provide a means of determining the reliability of, for example, a brake system, which may be required to ensure safe operation of the conveyor, in other words, the stated design standards do not provide a means to assess the reliability of the safety systems. As a result, specifications in tender documents never quantitatively address the issue of safety. Safe operation of belt conveyors is, however, a topic that must never be overlooked.
The reasons for this include:

1. Belt conveyors have many rotating components like idler rolls, pulleys, flywheels, and brake discs that do not only store high levels of kinetic energy but are also able to catch human clothing, hair, and arms.
2. The high tension apparent in the belt is a source of elastic energy, also called potential energy. Although the belt is designed to with stand these tensions, belt rupture may nonetheless occur. When it does, all the potential energy is released and causes the belt to behave highly unpredictably. There are reports of a ruptured belt wiping out a substantial part of the conveyor's

structure. If people are around when the belt breaks then this leads to a dangerous situation.

3. A serious downhill conveyor may be regenerative. Regenerative belt conveyors rely on their drive and brake systems as far as safety is concerned. If the drive system does not function properly then a normally serious sized brake is required to stop the conveyor. If that brake fails, the belt speeds up to very high velocities leading to dangerous situations as, for example, overloaded receiving chutes.
4. Man-carrying conveyors have two locations where personnel are able to move onto and off the conveyor. If an individual misses the exit, possibly because he fell asleep, or any other reason, then all kinds of safety measures come into play. The last measure is activating the brakes to stop the conveyor. If that brake fails, injuries or casualties may result.

Design of belt conveyor components that fulfill safety functions is therefore very important. Unfortunately, design standards for bulk material belt conveyors do not address functional safety issues. However consideration of this question will help in solving many issues related to possible damage of equipment and related loss of money and also to avoid fatal cases in accidents.

3.5.2 Belt conveyor safety

In the literature there are several authors who have discussed belt conveyor safety. Some introduce new equipment, others intelligent control systems. For example, Miguel Angel Reyes presents a wireless system to improve miner safety (Miguel Angel Reyes et al., 2014). Hou describes a control strategy for braking systems using brake discs and calipers for downhill belt conveyors. He states that this strategy enhances reliability of braking systems of belt conveyors (Hou et al., 2011). These and other authors address questions of belt conveyor safety and reliability. However, they do not explain how to measure safety or reliability and how to prove that, after application of wireless technology or a special control strategy for brakes, the belt conveyor becomes more reliable and safer. The concept of functional safety gives an answer to these questions. Unfortunately there are no papers investigating functional safety of belt conveyors. Functional safety is a "part of the overall safety relating to the Equipment Under Control (EUC) and the EUC control system that depends on the correct functioning of the electrical/electronic/programmable electronic (E/E/PE) safety-related systems and other risk reduction measures” (IEC 61508-4 2010). This model is well known in nuclear, chemical, civil and other branches of engineering. It was shown already in this Chapter for passenger conveyors. However it has not yet been applied to estimation of reliability in belt conveyors.

Stout et al. investigated issues with occupational safety in the mining industry (Stout et al., 2002). They noticed progress in reducing the occupational injuries over years. For instance, over 16600 US miners died during the five-year period from 1911 to 1915. This is 3300 deaths per year. During the five-year period 1996 to 2000, 429 miners died, just over 85 deaths per year. From 1911 through 1997 the rate of deaths per 100 000 miners plunged from well over 300 down to around 30. The catastrophes that happened at the beginning of the twentieth century led to a sweeping change and huge strides were made in the development of preventive strategies, including legislation and regulation (Stout et al., 2002). New safety standards (or amendments to standards) continue to appear every year in this area.

The search for related standards on belt conveyors' safety reveals many standards such as ISO 340 (Conveyor belts—Laboratory scale flammability characteristics - Requirements and test method), NEN-EN 620 + A 1 (Continuous handling equipment and systems—Safety and EMC requirements for fixed belt conveyors for bulk materials), NEN-EN 12882 (Conveyor belts f or general purpose use—Electrical and flammability safety requirements) and others. However there are no specific standards that contain information about SIL determination or risk assessment for belt conveyors. There is one common international standard of functional safety: IEC 61508 'Functional safety of electrical/electronic/programmable electronic (E/E/PE) safety-related systems'. As was stated in Chapter 2, standard IEC 61508 however, does not specify the safety integrity levels required for specific applications, called sector applications in the standard. These should be based on detailed information and knowledge of the sector application. Therefore it is necessary to develop the specification of SILs for belt conveyors. This is even more important when taking into account that belt conveyors are not only used for the transportation of mining products, but also for the transportation of people.

Another issue is insurance. If the owner of a machine like a belt conveyor, advises an insurance company that the conveyor has safety-related systems with SIL1, SIL2 and SIL3 levels, his premiums are likely to be lower as the insurer has a deeper insight into the reliability level of the machine. When the owner of the machine has documentary proof of the appropriate safety level of the machine, he is protected in case of an accident, even if fatal.

Further reliability analysis of braking system of belt conveyors in the concept of functional safety is given in the paper of Lodewijks & Rogova (Lodewijks and Rogova, 2014).

3.6 Conclusions

In this Chapter, the necessity of redundancy for a braking system of public service moving walks with described operating conditions was shown by using the functional safety concept. Conclusions of this Chapter are listed as follows:

1. Analytical formulas available in IEC 61508 are not applicable for PFD_{avg}/PFH calculation of systems with non-constant failure rates
2. Only simplified approximate reliability assessment was conducted to obtain PFH values of a braking system for seven test intervals. Obtained PFH values did not show correspondence to SIL2.
3. Proposed diagnostic system allowed to increase diagnostic coverage of a braking system
4. Calculation of PFH value after applying redundancy showed correspondence to SIL3 for 3 years and SIL 2 during 3-4 years of operation, which indicated significant reliability enhancement.
5. Design standards for bulk material belt conveyors should address functional safety issues
6. Decision to apply redundancy was made in accordance to functional safety concept on the basis of SIL-requirements as a criterion of not sufficient reliability of a braking system. Therefore this Chapter answered to the second research question: *How can the functional safety concept be used as a criterion for applying redundancy of a braking system of moving walks?*

Conducted analysis showed that analytical formulas of reliability assessment presented in IEC 61508 are not applicable for PFD_{avg}/PFH calculation of 1oo2 redundancy architecture with non-constant failure rates. Therefore the necessity of development of new analytical formulas of PFD_{avg}/PFH calculation for M-out-of-N redundancy architecture with non-constant failure rates was shown. These analytical formulas will be presented in Chapter 4.

References

Abernethy, R.B. (2004) *An overview of Weibull analysis, Chapter1. In: The new Weibull handbook.* 5th edn. North Palm Beach, Florida: Robert B. Abernethy, pp.1-11.

Al-Sharif, L. (2004). Intelligent Braking Systems for Public Service Escalators. *Proc. 1st International Conference for Building Electrical Technology Professional Network (BETNET)*, Hong Kong, China.

Balzer-Apke, L., Lange, D., Neumann, S., Pietz, A. (2003). Kone Corporation, assignee. Method for regulating the brake(s) of an escalator or a moving walkway. United States patent US 6,520,300 B2. 2003 Feb 18.

European Committee for Standardization (CEN) (2010) *EN 115-1+A1. Safety of escalators and moving walks – Part1: Construction and installation.*

Fedorov, Y.N. (2008). *APCS Engineering Handbook: design and development*. Moscow: Infra-Ingeneriya, Russian.

Gonzalez Alemany, M.A, Florez Castro, A., Ojeda Arenas, J., Rodriguez Rodriguez, E., Moran Garcia, E., Mendiolagoitia Juliana, J. (2013). Thyssenkrupp Elevator Innovation Center, S.A., assignee. Braking system for escalators and moving walks. United States Patent Application Publication US 2013/0153362 A1. 2013 Jun 20.

Hou, Y., Xie, F., Huang F. (2011), "Control strategy of disc braking systems for downward belt conveyors", *Mining Science and Technology (China)* 21, pp. 491-49.

International Electrotechnical Commission (IEC) (2004) *IEC 61511-1. Functional safety – Safety instrumented systems for the process industry sector. Part 1: Framework, definitions, system, hardware and software requirements.*

International Electrotechnical Commission (IEC) (2004*) IEC 61511-3. Functional safety – Safety instrumented systems for the process industry sector. Part 3: Guidance for the determination of the required safety integrity levels.*

International Electrotechnical Commission (IEC) (2005) IEC 62061. Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems.

International Electrotechnical Commission (IEC) (2006) *IEC 61078. Analysis techniques for dependability – Reliability block diagram and boolean methods.*

International Electrotechnical Commission (IEC) (2008) *IEC 61649. Weibull analysis.*

International Electrotechnical Commission (IEC) (2010) *IEC 61508-1. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1: General requirements.*

International Electrotechnical Commission (IEC) (2010) *IEC 61508-4. Functional safety of electrical/electronic/programmable electronic safety-related system. Part 4: Definitions and abbreviations.*

International Electrotechnical Commission (IEC) (2010) *IEC 61508-5. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 5: Examples of methods for the determination of safety integrity levels.*

International Electrotechnical Commission (IEC) (2013) *IEC 61508-6. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3.*

International Organization for Standardization (ISO) (2013) *ISO 22201-2. Lifts (elevators), escalators and moving walks – Programmable electronic systems in safety related applications – Part 2: Escalators and moving walks (PESSRAE).*

Kübler Group (2013) Villingen-Schwenningen: Encoders for Functional Safety, Operating Manual. Available at: http://www.clrwtr.com/PDF/Kubler/Kuebler-Sendix-SIL-Manual.pdf (Accessed 18 October 2016).

Kuo, W., Prasad, V.R., Tillman, F.A., Hwang, C.-L. (2001). *Optimal reliability design. Fundamentals and applications*. Cambridge: Cambridge university press.

Limpert, E., Stahel, W.A., Abbt, M. (2001). 'Lognormal Distributions across the Sciences: Keys and Clues'. *BioScience*, 51(5), pp.341-352.

Lodewijks, G. (1995), Rolling Resistance of Conveyor Belts, *Bulk Solids Handling*; 15, pp.15-22.

Lodewijks, G. (2002), 'Two Decades Dynamics of Belt Conveyors', *Bulk Solids Handling*, 22, pp.124-132.

Lodewijks, G., Rogova, E. (2014). Safety integrity level requirements in the design of belt conveyors. Proc. *Conference on Belt Conveyor Safety (SafeCon)*. Boksburg, South Africa, 1-15.

Los Angeles World Airports. (2011). Guide Specification. Section14 32 00 - moving walks. In: Design and Construction Handbook; p.1.

Mccann, M., Zaleski, N. (2006). *Deaths and injuries involving elevators and escalators. Deaths and injuries involving elevators or escalators*, 3rd edn. The Center to Protect Workers' Rights.

Reyes, M.A., King, G.W., Miller, G.G. (2014), Intelligent Machine Guard Monitoring: A wireless system to improve miner safety, *IEEE Industry Applications Magazine,* Mar-Apr 2014.

Rogova, E., Lodewijks, G. (2015) 'Braking system redundancy requirements for moving walks', *Reliab Eng Syst Safety*, 133, pp.203–211.

Rogova, E.S. (2012). *Risk analysis of technological system in Interlock system conception for ITER*. Manual for APCS engineers. Moscow: Typography NRNU MEPhI, Russian.

Scott Tyson. A. (2010). Metro escalator brake, maintenance problems widespread. The Washington post. 2010 Nov 14.

Selwyn. S., Kesavan. R. (2012). 'Reliability Analysis of Sub Assemblies for Wind Turbine at High Uncertain Wind', *Advanced Materials Research,* (433-440), pp.1121-1125.

Stout, I.N., Linn, H. I. (2002), 'Occupational injury prevention research: progress and priorities', *Injury Prevention,* 8 (sup.4): pp. 9-14.

Tavakkoli-Moghaddam, R., Safari, J., Sassani, F. (2008). 'Reliability optimization of series-parallel systems with a choice of redundancy strategies using a genetic algorithm', *Reliab Eng Syst Safety*, 93(4), pp.550-556.

Chapter 4

Analytical formulas of PFD$_{avg}$ and PFH calculation for systems with non-constant failure rates[*]

Chapters 1-3 showed that most analytical formulas developed for PFD$_{avg}$ (the average probability of failure on demand) and PFH (average frequency of dangerous failures per hour) calculation assume a constant failure rate. This assumption does not necessarily hold for system components that are affected by wear. This Chapter presents methods of analytical calculations of PFD$_{avg}$ and PFH for an M-out-of-N redundancy architecture with non-constant failure rates, and demonstrates its application in a case study. The method for the PFD$_{avg}$ calculation is based on the ratio between cumulative distribution functions and includes forecasting of PFD$_{avg}$ values with a possibility of update of failure rate function. The approach for the PFH calculation is based on simplified formulas and the definition of PFH. In both methods a Weibull distribution, introduced in Chapter 2, is used for a characteristics of the system behaviour. The PFD$_{avg}$ and PFH values are obtained for low, moderate and high degradation effects and compared with the results for the exponential distribution.

This Chapter is structured as follows. Section 4.1 describes the problem of reliability assessment of M-out-of-N redundant systems affected by wear. Section 4.2 explains the basic assumptions, the principle of PFD$_{avg}$ calculation for systems with non-constant failure rates and compare failure rates for low, moderate and high degradation effects. Section 4.3 contains formulas for PFD$_{avg}$ forecasting and the possible extensions of the formulas of PFD$_{avg}$

[*] The Chapter is based on E. Rogova, G. Lodewijks, M.A. Lundteigen (2017)

calculation. PFH formulas are obtained in Section 4.4. In Section 4.5 a simple subsystem is considered. Results obtained by using the developed and exact formulas of PFD_{avg} calculation, and results obtained by the new formulas of PFH calculation are presented and compared. These numerical results are obtained for low, moderate and high degradation effects and also compared with constant failure rates (exponentially distributed probability of failure). Section 4.6 discusses assumptions and limitations of the proposed formulas. The last section contains the conclusions.

4.1 Reliability quantification of M-out-of-N redundant systems affected by wear

There are many systems for which the failure rates of components can be considered as approximately constant. The assumption is valid e.g. for many electronic and electrical components, including programmable controller modules. A constant failure rate may also be assumed even for some mechanical components, if the effect of degradation is low.

The failure rate of repairable systems (or more precisely, the rate of occurrence of failures) often follows the well-known bathtub curve model (Figure 2.3). The model identifies three main regions, the first one is the region with infant mortality failures (decreasing failure rate), in the middle - the constant failure rate (when the item is regarded as being in the useful life period) and the wear-out period (where the failure rate is increasing). The failure rate of the useful life period can be calculated on the basis of assuming exponentially distributed time to failure. The Weibull distributed time to failure can be used to model all three regions.

The failure rates are important input data to the quantification of reliability, for example in relation to safety-critical systems (SCS) and associated safety-critical functions. IEC 61508, the most widely adapted standard for design of SCSs, specifies two possible reliability measures: Average Probability of Failure on Demand (PFD_{avg}) for low-demand mode systems and Average Frequency of Dangerous Failures per Hour (PFH) for high/continuous demand mode systems (IEC 6150,8 2010). PFD_{avg} and PFH values are usually calculated to verify the reliability against safety integrity level (SIL) requirements. Four SIL levels have been proposed in IEC 61508, along with an associated range for the required PFD_{avg} and PFH values.

The PFD_{avg}/PFH may be calculated on the basis of several reliability assessment methods: simplified formulas (Rausand, 2014, Jin et al., 2013, Hauge et al., 2010), IEC 61508 formulas, generalized analytical expressions (Chebila and Innal, 2015, Jin et al., 2013), Markov methods and Petri nets (Rausand, 2014). Common for many of the methods is the assumption about constant failure rate. For example, the formulas proposed in IEC 61508 for PFD_{avg} and PFH assume constant failure rate of all involved components. The same is the case for formulas provided by IEC 62061, a standard that is based on IEC 61508 but directed to machinery control systems (IEC 62061, 2005). Other methods allow relaxation of the constant failure rate assumption (along with assumptions about e.g. constant repair rates): for example, Petri Nets and block diagrams combined with Monte Carlo Simulations.

However “simplified formulas are still preferred by most practitioners, due to their simplicity” (Jin et al., 2013), but unfortunately few attempts have been made to include non-constant failure rate assumption. Since many SCS functions are split into subsystems that can include both electronic/electrical components (which do not reach the wear-out period before being replaced) as well as mechanical components such as valves (which reach the wear-out period), it would be an advantage to have simplified formulas for both scenarios.

The main purpose of this Chapter is therefore to develop simplified formulas for PFD_{avg} and PFH for SCS subsystems with redundancy, assuming that the failure rates are non-constant. The redundancy level may vary, and the term M-out-of-N is used here to denote how many (M) out of the N redundant components that must function in order for the subsystem to carry out the safety function. The formulas assume that the redundant components are of identicial type (with same failure rate and failure rate assumption). The proposal for PFD_{avg} calculation builds on ideas first developed in a master thesis by Jigar (Jigar 2013), and which were further elaborated in Rogova et al. (2015).

Based on the literature review, it is assumed in this dissertation that the Weibull distribution is one of the best choices for a description of system components with degradation (i.e. with non-constant failure rate). Many researchers (Santos et al., 2014, Dersin et al., 2008, Kumar and Jackson, 2009, Chudoba, 2011 and others) choose Weibull as a distribution for a characteristics of degrading behavior. A Weibull analysis has several advantages such as reasonably accurate failure analysis, a failure forecast with very small samples, and a simple and useful graphical plot of the failure data. There are data bases with Weibull shape factors α and characteristic life η parameters for all main types of mechanical equipment that makes engineering calculations of reliability very suitable (Rogova and Lodewijks, 2015). However, a failure rate function is not the only solution for degrading components, and the formula of constant failure rate dependent on number of cycles suggested by ISO 13849 (ISO 13849-1, 2015) can be used in some cases.

A challenge with PFD_{avg} calculations is the assumption of regular functional testing and regular renewal. Simplified formulas with constant failure rate assumption often regard each functional test as perfect, meaning that the state of the system is as good as new after the test. With a component being in the wear-out period, the same assumption about renewal cannot be made. The PFD_{avg} calculated for the first test interval would therefore not be the same as the PFD_{avg} calculated for the subsequent intervals.

For calculation of PFH the effects of regular testing are less important than for low-demand systems, as the effects of a failure of a SCS in the high-demand mode would give an immediate danger. In the calculation of PFH it is therefore more important to decide on a reasonable time interval for which an average system failure frequency can be regarded as representative, and it is recognized that the PFH will change if the time interval changes.

4.2 Approach to derive PFD_{avg} formulas

The approach to derive a set of simplified formulas for the PFD_{avg} for the first and subsequent test intervals make use of the idea in Jigar (Jigar, 2013). This idea is based on the ratio between Weibull cumulative distribution functions (CDFs): Weibull CDFs for 1-out-of-k and for 1-out-of-n architectures ($k \geq n$): $F_k(t)=1-\exp(-\lambda_k t)^{\alpha}$ and $F_n(t)=1-\exp(-\lambda_n t)^{\alpha}$. $F_k(t)$ can be expressed by ratio between mean values of distributions ($F_k(t)$ and $F_1(t)$) and by $F_1(t)$ for 1oo1 architecture. The ratio between mean values of distributions ($F_k(t)$ and $F_1(t)$) is a "multiplier" A(t), that exists in each time point (Jigar, 2013).

$$\begin{cases} \frac{F_k(t)}{F_n(t)} = \frac{1-e^{-(\lambda_k t)^{\alpha}}}{1-e^{-(\lambda_n t)^{\alpha}}} \approx \frac{(\lambda_k)^{\alpha}}{(\lambda_n)^{\alpha}} = \left(\frac{\mu_n}{\mu_k}\right)^{\alpha} \\ F_{1ook}(t) = F_k(t) = \frac{1}{A(t)} \cdot F_{1oo1}(t) \end{cases} \tag{4.1}$$

where μ is the mean of the distribution; λ and α - Weibull scale and shape parameters, respectively (Jigar, 2013).

The formula for exact calculation of CDF $F_k(t)$ for 1-out-of-k architecture:

$$F_k(t) = \mathrm{F(t)}^k$$

The approximate CDF $\tilde{F}_k(t)$ for 1-out-of-k architecture can be written:

$$\begin{cases} \tilde{F}_k(t) = [A_k \cdot (\mathrm{F(t)})^{k-1}] \cdot F_{1oo1}(t) \\ A_k = \left(\frac{\mu_1}{\mu_k}\right)^{\alpha} \end{cases} \tag{4.2}$$

Therefore based on the obtained formula of $\tilde{F}_k(t)$ for 1ook (Equation 4.2), PFD$_{\mathrm{avg}}$ for a single component for the first test interval is obtained as follows (Jigar, 2013):

$$PFD_{avg,k_1} = \frac{1}{\tau}\int_0^{\tau} \tilde{F}_k(t)\ \mathrm{dt}$$

$$PFD_{avg,k_1} = \frac{A_k}{\tau}(1-e^{-(\lambda\tau)^{\alpha}})^{k-1}\int_0^{\tau}(1-e^{-(\lambda t)^{\alpha}})\,dt \tag{4.3}$$

On the basis of Equations 4.1-4.3 the final formulas for a multiplier A$_k$ and the PFD$_{\mathrm{avg,k1}}$ for the first test interval τ (for the architecture MooN) can be obtained as follows (Jigar, 2013):

$$\begin{cases} PFD_{avg,k_1} \approx \binom{N}{N-M+1}\frac{A_k}{\alpha+1}(\lambda\tau)^{\alpha k} \\ A_k = \left(\frac{\mu_1}{\mu_k}\right)^{\alpha} = \left[\sum_{x=1}^{k}\binom{k}{x}(-1)^{x+1}x^{-\frac{1}{\alpha}}\right]^{-\alpha} \end{cases} \tag{4.4}$$

where k=N-M+1 and k$_1$ means the first test interval.

It is important to notice that all these formulas are derived here in the assumption of equal and identical channels.

4.*2.1 Failure rate function and the PFD*$_{avg}$ *formula*

The failure rate of a system/component with degradation is not a constant value, it is a function depending on time. The Weibull CDF and corresponding failure rate function are thereby, calculated by the formula (Bertsche, 2008):

$$\begin{cases} F(t) = 1 - e^{-\left(\frac{t}{\eta}\right)^{\alpha}} \\ \lambda(t) = \frac{\alpha t^{\alpha-1}}{\eta^{\alpha}} \end{cases} \tag{4.5}$$

where α – Weibull shape parameter; η - Weibull Characteristic Life (in hours).

Jigar (Jigar, 2013) and Rausand and Hoyland (Rausand and Hoyland, 2004), however suggest using other notation:

$$\begin{cases} F(t) = 1 - e^{-(\lambda t)^{\alpha}} \\ \lambda = \frac{1}{\eta} \\ z(t) = \frac{f(t)}{R(t)} = \frac{\alpha t^{\alpha-1}}{\eta^{\alpha}} \end{cases} \tag{4.6}$$

where λ – scale parameter, f(t) – probability density function, R(t)- reliability (survivor) function, z(t) – failure rate function.

Equations 4.5-4.6 demonstrate a different notation: λ(t) is a failure rate function in the system of Equations 4.5 and a scale parameter (λ) for the system of Equations 4.6. It is important to notice that the scale parameter is not equal to the failure rate (it is correct only for α=1, when the failure rate is constant). In this thesis the notation z(t) is used as a failure rate (hazard) function. Table 4.1 shows numerical results obtained by using the failure rate function z(t) for three mechanical components (sources of Weibull data: Baek-Ju, 2012 and Bertsche, 2008).

Table 4.1: Failure rates for mechanical components.

Failure rate	**Solenoid valve (Low degradation)**	**Bearings (Moderate degradation)**	**Gears (High degradation)**
z(t=1h)	$2.13\cdot10^{-4}$	$3.86\cdot10^{-4}$	$8.27\cdot10^{-5}$
z(t=8760h)	$5.29\cdot10^{-4}$	$1.00\cdot10^{-3}$	$1.18\cdot10^{-1}$

Based on the data given in Table 4.1, the failure rate value for a solenoid valve can be considered as approximately constant: $\lambda \approx 3.7 \cdot 10^{-4}$=const (mean value of z(t=1h) and z(t=8760h)) for the test interval τ=8760 hours (1 year). However the failure rate values of bearings and gears cannot be approximated by constant values which proves that a constant failure rate can be applied only for some cases with a weak degradation (α≈1) during one test interval. Obtained values of the failure rates also support a concept of failure rate function for mechanical components with significant degradation. For gears and bearings a constant failure rate cannot be applied. An increase of the test interval and/or an increase of the deterioration process may result in a value that is even further away from the correct value.

Taking into account the formula of a time-dependent failure rate function, the system of Equations 4.4 can be transformed to a system of Equations 4.7:

$$\begin{cases} PFD_{avg,k1} \approx \binom{N}{N-M+1} \frac{A_k}{\alpha+1} \left(\frac{z(\tau)\tau}{\alpha}\right)^k \\ A_k = \left(\frac{\mu_1}{\mu_k}\right)^\alpha = \left[\sum_{x=1}^{k} \binom{k}{x} (-1)^{x+1} x^{-\frac{1}{\alpha}}\right]^{-\alpha} \end{cases} \quad (4.7)$$

where z(τ) is a failure (hazard) rate function.

Compared to Equation 4.4, that contains λ as a scale parameter from Equation 4.6, Equation 4.7 includes a Weibull failure rate function.

The definition of PFD_{avg} given by (Rausand and Hoyland, 2004) is used here as a correct method for calculation of PFD_{avg} value. In this Chapter it is called the "exact" method:

$$\begin{cases} PFD_{MooN} = 1 - \frac{1}{\tau} \int_0^\tau R_{MooN}(t) dt \\ R_{MooN} = \sum_{i=M}^{N} \binom{N}{i} R^i \cdot (1-R)^{N-i} \\ R(t) = e^{-\left(\frac{t}{\eta}\right)^\alpha} \end{cases} \quad (4.8)$$

The system of Equations 4.8 contains integrals that cannot be solved analytically. These integrals can be solved by using numerical methods (for instance, the trapezoid method).

4.3 The PFD$_{avg}$ forecasting and extended formulas

4.3.1 Forecasting

As was described in Section 4.2, the formula for the PFD$_{avg}$ calculation is valued only for the first test interval. However, consideration of the i-th test interval [(i-1)τ; iτ] is even more important for some applications. Prognosis for PFD$_{avg,ki}$ in the i-th test interval k$_i$ can be made by using the equation suggested by Jigar (Jigar, 2013):

$$PFD_{avg,ki} = \binom{N}{N-M+1}\frac{A_k \cdot \lambda^{\alpha}}{(1+\alpha)\cdot\tau}\left[(i\tau)^{\alpha+1} - ((i-1)\tau)^{\alpha+1}\right] \cdot \left[(\lambda i\tau)^{\alpha} - (\lambda(i-1)\tau)^{\alpha}\right]^{k-1} \quad (4.9)$$

However such forecasting depends on the Weibull scale parameter λ (Equation 4.6) and does not include the failure rate function z(t). Inclusion of the failure rate function in the system of equations (Equation 4.7) gives new possibilities to the formula for PFD$_{avg}$ forecasting. Taking into account the formula of the failure rate function (Equation 4.6), Equation 4.9 should be also transformed. Therefore, the current PFD$_{avg,ki}$ value for the i-th test interval (t=iτ) is obtained for the architecture M-out-of-N with account of the failure rate function:

$$\begin{cases} PFD_{avg,ki} = \binom{N}{N-M+1}\frac{A_k}{(1+\alpha)}\left(\frac{z(\tau)\cdot\tau}{\alpha}\right)^{k} \cdot \left[i^{\alpha+1} - (i-1)^{\alpha+1}\right] \cdot \left[i^{\alpha} - (i-1)^{\alpha}\right]^{k-1} \\ A_k = \left(\frac{\mu_1}{\mu_k}\right)^{\alpha} = \left[\sum_{x=1}^{k}\binom{k}{x}(-1)^{x+1}x^{-\frac{1}{\alpha}}\right]^{-\alpha} \end{cases} \quad (4.10)$$

It worth to note that prognosis for current PFD$_{avg,ki}$ value is based on the assumption that no changes are made for the CDF. All changes and updates of CDF has to be done before the test interval *i*. For the first test interval *i=1* Equation 4.10 is transformed to Equation 4.7.

Sometimes during the proof test, “a carefully planned periodic test, which is designed to reveal all DU faults of each channel of a safety loop” (Rausand, 2014), additional number of operating cycles is required that can significantly reduce the remaining number of operating cycles for the component. This should be taken into account for further calculations of PFD$_{avg}$ and PFH by updating the failure rate function. The approach for PFD$_{avg}$ and PFH forecasting described in this Chapter allows to conduct different kinds of updates of the failure rate function z(t) based on Equation 4.6. The unified approach of the failure rate function update is difficult to develop because the updating procedure should be specified for the component.

Engineers also need to observe the system entirely: if the specified SIL is not achieved for the function, it is necessary to consider reducing the test intervals, replace individual components, or carry out a root cause analysis with the aim to reduce the occurrence of specific failure causes. The test interval may be updated in accordance to Vatn (Vatn, 2006) or the approach advocated by SINTEF (Hauge and Lundteigen, 2008).

The importance of using the failure rate function in the presented formulas (Equation 4.10) is especially evident when several test intervals are under consideration. In this case the $PFD_{avg,ki}$ value calculated after several test intervals, can be compared to the corresponding $PFD_{avg,ki}$ value after updating the failure rate function (due to repair/replacement/increase of number of cycles during the proof test). Equation 4.9 does not give this possibility.

4.3.2 Extended PFD_{avg} formulas

The extended formulas of the developed method include the diagnostic coverage DC, dangerous undetected DU failures, and common cause failures CCF with a β-factor-model (dangerous detected DD failures do not make a big contribution to PFD_{avg}). It is important to note that the Weibull failure rate function (Equation 4.6) does not apply for describing the whole component failures (global failure rate). The Weibull failure rate function is used here only for dangerous failures and does not characterize safe failures.

The formula for the PFD_{avg} calculation in a system of Equations 4.9 can be extended (here, a pragmatic assumption is made regarding the CCFs, assuming that the rate of CCFs is constant in each test interval):

$$PFD_{avg,k_1} \approx \binom{N}{N-M+1} \cdot \frac{A_k}{\alpha+1}\left(\frac{(1-\beta)z_{DU}(\tau)\cdot\tau}{\alpha}\right)^k + PFD_{CCF} \qquad (4.11)$$

where CCF part is included as an additional summand; z_{DU}=(1-DC)· z_D (z_D is rate of dangerous failures, D=DD+DU).

PFD_{CCF} is a contribution from CCF. This addend is a “virtual CCF element” (Rausand, 2014) that represents dependent failures. For constant failure rates this contribution is approximately estimated as follows (Rausand, 2014):

$$PFD_{CCF} = \frac{\beta\lambda_{DU}\cdot\tau}{2} \tag{4.12}$$

PFD$_{\text{CCF}}$ for non-constant failure rates modeled by Weibull-distribution has to be obtained as follows:

$$PFD_{CCF} = 1 - \frac{1}{\tau}\int_0^{\tau} e^{-\frac{\beta\cdot t\cdot z_{DU}(t)}{\alpha}} dt = 1 - \frac{1}{\tau}\int_0^{\tau} e^{-\frac{\beta\cdot(1-DC)\cdot t^{\alpha}}{\eta^{\alpha}}} dt \tag{4.13}$$

In case of approximation by first two addends, the value of PFD$_{\text{CCF}}$ can be obtained as follows:

$$PFD_{CCF} = \frac{\beta\cdot z_{DU}(\tau)\cdot\tau}{\alpha(\alpha+1)} \tag{4.14}$$

The Equation 4.14 transforms to Equation 4.12 for α=1 (exponential case).

By using Equation 4.11 and Equation 4.14, the formula of PFD$_{\text{avg}}$ calculation for the first test interval with account of CCF is obtained as follows:

$$PFD_{avg,k_1} \approx \binom{N}{N-M+1}\cdot\frac{A_k}{\alpha+1}\left(\frac{(1-\beta)z_{DU}(\tau)\cdot\tau}{\alpha}\right)^k + \frac{\beta\cdot z_{DU}(\tau)\cdot\tau}{\alpha(\alpha+1)} \tag{4.15}$$

Formula of PFD$_{\text{CCF}}$ calculation for PFD$_{\text{avg}}$ forecasting is calculated as follows:

$$PFD_{CCF} = 1 - \frac{1}{\tau}\int_{(i-1)\tau}^{i\tau} e^{-\frac{\beta\cdot t\cdot z_{DU}(t)}{\alpha}} dt = 1 - \frac{1}{\tau}\int_{(i-1)\tau}^{i\tau} e^{-\frac{\beta\cdot(1-DC)\cdot t^{\alpha}}{\eta^{\alpha}}} dt \approx$$
$$\approx \frac{\beta z_{DU}(\tau)\cdot\tau}{\alpha(\alpha+1)}\cdot\left[i^{\alpha+1} - (i-1)^{\alpha+1}\right] \tag{4.16}$$

Therefore, Equation 4.10 for PFD$_{\text{avg}}$ forecasting should be extended with account of DU and CCF:

$$PFD_{avg,ki} = \binom{N}{N-M+1}\frac{A_k}{(1+\alpha)}\left(\frac{(1-\beta)\cdot z_{DU}(\tau)\cdot\tau}{\alpha}\right)^k\cdot\left[i^{\alpha+1} - (i-1)^{\alpha+1}\right]\cdot\left[i^{\alpha} - (i-1)^{\alpha}\right]^{k-1} + \frac{\beta z_{DU}(\tau)\cdot\tau}{\alpha(\alpha+1)}\cdot\left[i^{\alpha+1} - (i-1)^{\alpha+1}\right] \tag{4.17}$$

Calculation of the CCF for the PFD$_{\text{avg}}$ forecasting is more complicated than for the first test interval. Equation 4.17 takes into account the increase of the CCF contribution to the PFD$_{avg}$ value during several test intervals. In addition, in case of lack of repair/replacement after the test interval, degradation is continuing and the value of the β-factor can change. It means that strong degradation of components in channels of M-out-of-N architecture can probably lead to an increase of the mutual influence between channels. However, for identical channels with the same Weibull shape parameters β-factor is still constant (Pozsgai et al., 2002).

The system of Equations 4.8 for the exact calculation of the PFD$_{avg}$ with account of DU and CCF becomes:

$$\begin{cases} PFD_{MooN} = 1 - \frac{1}{\tau}\int_0^\tau R_{MooN}(t)dt \\ R_{MooN} = \left(\sum_{i=M}^{N}\binom{N}{i}R^i \cdot (1-R)^{N-i}\right) \cdot R_{CCF} \\ \qquad = \left(\sum_{i=M}^{N}\binom{N}{i}e^{-\frac{(1-\beta)z_{DU}(t)\cdot t\cdot i}{\alpha}} \cdot \left(1 - e^{-\frac{(1-\beta)z_{DU}(t)\cdot t}{\alpha}}\right)^{N-i}\right) \cdot e^{-\beta z_{DU}(t)\cdot t} \end{cases} \tag{4.18}$$

4.4 Derivation of new formulas for PFH

PFH is the suggested reliability for safety-critical systems operating in the high-demand mode. The term PFH is somewhat confusing, as it is defined as the *Probability of having a dangerous Failure per Hour*. First, it is not common to assign a fixed time measure (here hours) for a frequency measure, and secondly the term probability in this context is somewhat unclear. The PFH is in the most recent version of IEC 61508 referred to as failure frequency (but the abbreviation PFH has been kept), and may be interpreted as the average ROCOF (rate of occurrence of failures) with respect to the contribution of dangerous (D) failures in a time interval. The PFH may therefore be defined as (Rausand, 2014):

$$PFH_G(0,\tau) = \frac{Mean\ number\ of\ DGFs\ in\ (0,\tau)}{\tau} \tag{4.19}$$

where DGF is the average dangerous group failures, i.e. the average frequency of failure of a safety-critical function or subsystem in the interval (0,τ). It may here be noted that the interval is not necessarily the same as the proof test interval, but in case of regular proof testing it may be easier to align the two.

The mean number of DGFs may (for forecasting) be determined by the expected number of D failures occurring in the interval (0, τ). If $N_G(\tau)$ is the number of DGFs, the PFH then becomes:

$$PFH_G = \frac{E[N_G(\tau)]}{\tau} \qquad (4.20)$$

If the interval τ is short (bearing in mind that the safety-critical systems are built for high reliability) it is reasonable to assume that either no or one failure occurs during this time period. It is therefore possible to make the following approximation about the mean number of group failures (Rausand, 2014):

$$E[N_G(\tau)] = 0 \cdot \Pr(N_G(\tau) = 0) + 1 \cdot \Pr(N_G(\tau) = 1) = \Pr(V(\tau) \geq N - M + 1) = \sum_{j=N-M+1}^{N} \Pr(V(\tau) = j) \qquad (4.21)$$

The important issue is to ensure that the interval τ is not longer than reasonable to fulfil the assumption underlying Equation 4.21.

Dangerous group failure occurs when at least N-M+1 of the N channels have dangerous faults in the same proof test interval (Rausand, 2014).

Under the assumption of identical and independent channels, it may be assumed that the number of channels *V(τ)* that fail in an interval τ, is binomially distributed, but instead of assuming exponentially distributed time to failure, it is proposed to use the Weibull distribution. This means that:

$$\Pr(V(\tau) = j) = \binom{N}{j}\left(1 - e^{-\frac{\tau \cdot z_D(\tau)}{\alpha}}\right)^{j} \cdot \left(e^{-\frac{\tau \cdot z_D(\tau)}{\alpha}}\right)^{N-j} \qquad (4.22)$$

where $F(\tau) = 1 - e^{-\frac{\tau \cdot z_D(\tau)}{\alpha}}$is the probability to fail (Weibull CDF) and $R(\tau) = e^{-\frac{\tau \cdot z_D(\tau)}{\alpha}}$ is the probability of surviving.

This means that the following expression for PFH can be obtained:

$$\mathrm{PFH}_G^{MooN} = \frac{E[N_G(\tau)]}{\tau} = \frac{1}{\tau} \cdot \sum_{j=N-M+1}^{N} \binom{N}{j}\left(1 - e^{-\left(\frac{\tau \cdot z_D(\tau)}{\alpha}\right)}\right)^{j} \cdot \left(e^{-\left(\frac{\tau \cdot z_D(\tau)}{\alpha}\right)}\right)^{N-j} \qquad (4.23)$$

For small $\frac{\tau \cdot z_D(\tau)}{\alpha}$: $\left(\frac{\tau \cdot z_D(\tau)}{\alpha}\right)^{j+1} \ll \left(\frac{\tau \cdot z_D(\tau)}{\alpha}\right)^{j}$ for all $j \geq 1$ (4.24)

This gives:

$$\mathrm{PFH}_G^{MooN} = \frac{1}{\tau} \cdot \sum_{j=N-M+1}^{N} \Pr(V(\tau) = j) \approx \frac{\Pr(V(\tau)=N-M+1)}{\tau} \quad (4.25)$$

To further simplify, the following approximations are introduced (Rausand, 2014):

$$1 - e^{-\frac{\tau \cdot z_D(\tau)}{\alpha}} \approx \frac{\tau \cdot z_D(\tau)}{\alpha};\ e^{-\frac{\tau \cdot z_D(\tau)}{\alpha}} \approx 1 \quad (4.26)$$

It is important to note that such approximation gives good accuracy only for small values of $\frac{\tau \cdot z_D(\tau)}{\alpha}$. If this value is not small, the better approximation can be obtained by including more addends. The numerical comparison of accuracy for different Weibull parameters is presented in Section "Calculation of PFH".

Taking into account Equation 4.23 and approximations presented in Equations 4.24-4.26, it is possible to get:

$$\mathrm{PFH}_G^{MooN} = \binom{N}{N-M+1} \cdot \left(\frac{\tau \cdot z_D(\tau)}{\alpha}\right)^{(N-M+1)} \cdot \tau^{-1} = \binom{N}{N-M+1} \cdot \left(\frac{z_D(\tau)}{\alpha}\right)^{(N-M+1)} \cdot \tau^{N-M} \quad (4.27)$$

If α=1, then Equation 4.27 is transformed to the Rausand formula (Rausand, 2014) of PFH calculation for SCS with constant failure rates and D failures:

$$\mathrm{PFH}_G^{MooN}(\alpha = 1) = \binom{N}{N-M+1} \cdot {z_D}^{(N-M+1)} \cdot \tau^{N-M} \quad (4.28)$$

If the channels are dependent, CCF should be included together with individual failures:

$$PFH = \binom{N}{N-M+1} \cdot \left(\frac{(1-\beta) \cdot z_D(\tau)}{\alpha}\right)^{(N-M+1)} \cdot \tau^{N-M} + \frac{\beta \cdot z_D(\tau)}{\alpha} \quad (4.29)$$

Taking into account CCF by using the PDS approach (Hauge et al, 2010), it is necessary to include additional summand PFH$_{\mathrm{CCF}}$:

$$PFH = PFH_{CCF} + PFH_D \approx \frac{C_{MooN} \cdot \beta \cdot z_D(\tau)}{\alpha} + \binom{N}{N-M+1} \cdot \left(\frac{z_D(\tau)}{\alpha}\right)^{(N-M+1)} \cdot \tau^{N-M} \quad (4.30)$$

where C_{MooN} is the corrections factor estimated based on expert judgement (Rausand, 2014).

Obtained formulas contain no forecasting. However despite proof testing policy, one may expect that the PFH(0, τ) would be different from PFH(τ, 2τ), PFH(2τ, 3τ) etc. due to continuing degradation. Therefore the forecasting formula can be proposed:

$$PFH\big((i-1)\tau, i\tau\big) = \frac{E[N_G(i\tau)] - E\big[N_G\big((i-1)\tau\big)\big]}{\tau} \tag{4.31}$$

On the basis of Equation 4.31 and taking into account Equations 4.21-4.26, the following formula of PFH prognosis for the interval ((i-1)τ; τ) can be obtained:

$$PFH\big((i-1)\tau, i\tau\big) = \binom{N}{N-M+1} \cdot \left(\frac{(1-\beta)z_D(\tau)}{\alpha}\right)^{(N-M+1)} \cdot \tau^{N-M} \cdot$$
$$\cdot \left(i^{\alpha\cdot(N-M+1)} - (i-1)^{\alpha\cdot(N-M+1)}\right) + \frac{\beta\cdot z_D(\tau)\cdot(i^{\alpha}-(i-1)^{\alpha})}{\alpha} \tag{4.32}$$

4.5 Case study

The case study was designed to demonstrate the applicability of the developed formulas of PFD_{avg} and PFH calculation for the first test interval and for PFD_{avg} and PFH forecasting to transport safety system with low, moderate and high degradation effects.

4.5.1 Calculation of PFD_{avg}

The system considered in this case study is a safety system of an hydraulic elevator. It consists of a motorized valve MV, a sensor of valve position PS and a fluid reservoir. When the hydraulic elevator goes down, the liquid should be removed from the reservoir to allow a piston to move down. If a motorized valve is stuck and the liquid cannot be removed from the reservoir, the elevator cannot go down. The sensor of valve position sends signals to the PLC that the valve is stuck. The PLC sends commands to open the redundant motorized valve MV1 to remove all the liquid from the reservoir and allow the elevator to go down to the first floor to free passengers/cargo. The simplified scheme of automation is shown in Figure 4.1. The safety-critical function for the safety system is: “Remove all the liquid from a cylinder to allow going down”. It is assumed here that SIL for this safety function was estimated as SIL2 (the procedure of determination of SIL-requirements was discussed in Chapter 3).

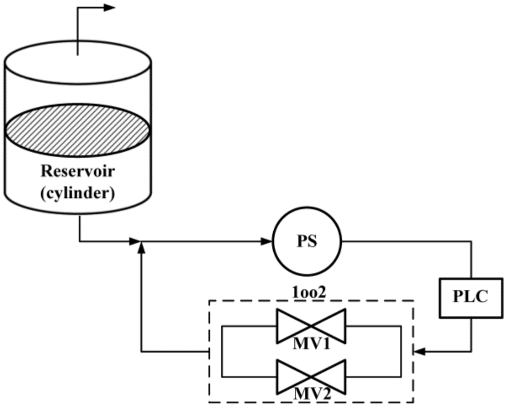


Figure 4.1: Scheme of automation.

The PFD_{avg} for a position sensor (Aschenbrenner, 2004) is $4.22\cdot10^{-5}$, failure rate is $9.63\cdot10^{-9}$ (h^{-1}). The PFD_{avg} of a PLC with basic configuration is estimated by Siemens (Siemens, 2014) as $1.7\cdot10^{-4}$, the failure rate is $3.88\cdot10^{-8}$ (h^{-1}). We consider several possible degradation modes for a motorized valve. Each degradation mode has its Weibull parameters. α=1.1 and η=150,000 h for the low degradation effect. For comparison we take also possible moderate (α=1.5, η=110,000 h) and high (α=1.7, η=80,000 h) degradation effect for this valve (see Tables 4.2-4.3). In the case of low degradation effect $PFD_{avg}(\tau=8760h)=2\cdot10^{-2}$, $PFH(\tau=8760h)=5.02\cdot10^{-6}$ for the SCS entirely, which is not sufficient for SIL2. These values of PFD_{avg} and PFH are calculated for the architecture 1oo1 (Equations 4.11 and 4.27) and summed with PFD_{avg} and PFH values of a position sensor and PLC.

The system reliability can be improved by applying redundancy (1-out-of-2) and diagnostics for the motorized valve (Figure 4.1). Taking into account that diagnostic coverage is approximately estimated as DC≈60%, the failure rate can be calculated as $z_{DU}(\tau=8760)=2.21\cdot10^{-6}$ per hour for the low degradation effect. Common cause failures are 2%. Using the extended PFD_{avg} formula (Equation 4.15), the PFD_{avg} values were obtained for a system after applying redundancy (Table 4.2).

Table 4.2: $PFD_{avg,k1}$(τ=8760h) values after applying 1oo2 redundancy for a valve.

Distribution	$PFD_{avg,k1}$	$PFD_{avg,k1}$ (exact)	Δ,%	$PFD_{avg,k1}$	$PFD_{avg,k1}$ (exact)	SIL
	Valves			System entirely		
Weibull (low degradation effect: α=1.1; η=150,000 h)	$2.60\cdot10^{-4}$	$2.59\cdot10^{-4}$	0.4	$4.72\cdot10^{-4}$	$4.71\cdot10^{-4}$	3
Weibull (moderate degradation effect: α=1.5; η=110,000 h)	$9.13\cdot10^{-5}$	$9.12\cdot10^{-5}$	0.1	$3.03\cdot10^{-4}$	$3.03\cdot10^{-4}$	3
Weibull (high degradation effect: α=1.7; η=80,000 h)	$8.79\cdot10^{-5}$	$8.78\cdot10^{-5}$	0.1	$3.00\cdot10^{-4}$	$3.00\cdot10^{-4}$	3

As shown in Table 4.2, after applying redundancy, PFD_{avg}(τ=8760) of subsystem “1oo2 valve redundancy” is appropriate for SIL-requirements (SIL2) for all degradation effects. Table 4.2 shows that the results obtained by using the analytical formula of PFD_{avg} calculation and exact formula are very close. The average difference between results $\Delta_{avg} = 0.2\%$.

By using Equation 4.17, it is possible to conduct PFD_{avg} forecasting for several test intervals (Table 4.3). For low degradation effects a motorized valve is degrading but still corresponds to SIL2 during the twelve test intervals (τ=8760h). For moderate degradation effects the number of test intervals where PFD_{avg} corresponds to SIL2 is nine. For high degradation effect we can see that PFD_{avg} is ok for SIL2 during six test intervals. All PFD_{avg} values are presented for a system entirely (together with PFD_{avg} for PLC and PS).

The results, demonstrated in Table 4.3, show degradation of a system with applied redundancy architecture during each proof test interval. It is also important to note that the large number of cycles (open-close) of a valve during the proof test can significantly increase PFD_{avg} value and therefore decrease the number of test intervals that correspond to the required SIL. If it is the case, the failure rate function should be updated and included to the calculations. The numerical results in Table 4.3 also demonstrate importance of using a failure rate function for degrading components, proof the applicability of Equation 4.17 for PFD_{avg} forecasting with account of DU and CCF failures.

Table 4.3: $PFD_{avg,ki}$ $(i\tau)$ prognosis for low, moderate and high degradation effects for 1oo2 architecture.

i	$PFD_{avg,ki}$ $((i-1)\tau, i\tau)$ $(\tau=8760h)$	SIL
	Low degradation effects	
1	$4.72 \cdot 10^{-4}$	3
2	$1.11 \cdot 10^{-3}$	2
3	$1.82 \cdot 10^{-3}$	2
...		
13	$1.03 \cdot 10^{-2}$	1
	Moderate degradation effects	
1	$3.03 \cdot 10^{-4}$	3
2	$7.12 \cdot 10^{-4}$	3
3	$1.38 \cdot 10^{-3}$	2
...		
10	$1.20 \cdot 10^{-2}$	1
	High degradation effects	
1	$3.00 \cdot 10^{-4}$	3
2	$8.25 \cdot 10^{-4}$	3
3	$1.89 \cdot 10^{-3}$	2
...		
7	$1.24 \cdot 10^{-2}$	1

4.5.2 Calculation of PFH

The same system can be considered also in a high-demand mode. Table 4.4 presents the numerical results of PFH calculations after applying redundancy (Equation 4.29) by using simplified formulas. These values are compared with PFH values obtained on the basis of full formulas (Equation 4.23) that give exact results without approximation.

Table 4.4: PFH(τ=8760h) values after applying 1oo2 redundancy for a valve.

Distribution	PFH Simplified formulas	PFH Full formulas	Δ, %	PFH Simplified formulas	PFH Full formulas	SIL
	Valves			System entirely		
Weibull (low degradation effect: α=1.1; η=150,000 h)	$7.40\cdot10^{-8}$	$7.35\cdot10^{-8}$	0.7	$1.22\cdot10^{-7}$	$1.22\cdot10^{-7}$	2
Weibull (moderate degradation effect: α=1.5; η=110,000 h)	$2.94\cdot10^{-8}$	$2.93\cdot10^{-8}$	0.3	$7.78\cdot10^{-8}$	$7.77\cdot10^{-8}$	3
Weibull (high degradation effect: α=1.7; η=80,000 h)	$3.08\cdot10^{-8}$	$3.07\cdot10^{-8}$	0.3	$7.92\cdot10^{-8}$	$7.91\cdot10^{-8}$	3

Obtained in Table 4.4 numerical results compared with the corresponding SIL (IEC 61508-1, 2010) for a system entirely by using simplified formulas. The difference in obtained SIL values for the same subsystem in high/continuous (Table 4.4) and low demand mode (Table 4.2) is a well-known phenomenon described by Rausand (Rausand, 2014).

Results obtained by simplified and full formulas of PFH calculation are very close for all degradation effects. The average difference between obtained results is very small: Δ_{avg}=0.4%. The simplified formulas use approximation. Therefore some systems with smaller values of scale parameters η can give less accuracy. In this case in accordance to Equation 4.26 the number of addends in Taylor series can be increased.

PFH forecasting is based on Equation 4.32. In Table 4.5 the results of calculations for PFH forecasting for the valves in 1oo2 architecture are presented.

Table 4.5: PFH (iτ) prognosis for low, moderate and high degradation effects for 1oo2 architecture.

i	PFH ((i-1)τ, iτ) (τ=8760h)	SIL
	Low degradation effects	
1	$1.22 \cdot 10^{-7}$	2
2	$2.16 \cdot 10^{-7}$	2
...		
9	$1.07 \cdot 10^{-6}$	1
	Moderate degradation effects	
1	$7.78 \cdot 10^{-8}$	3
2	$1.48 \cdot 10^{-7}$	2
...		
7	$1.25 \cdot 10^{-6}$	1
	High degradation effects	
1	$7.92 \cdot 10^{-8}$	3
2	$1.87 \cdot 10^{-7}$	2
...		
5	$1.35 \cdot 10^{-6}$	1

Table 4.5 shows that PFH values are increasing each test interval. For low degradation effects the system corresponds to SIL2 during eight test intervals. For moderate degradation effects – during six test intervals. For high

degradation effects system corresponds to SIL2 during 4 test intervals. In addition, in accordance to the described forecasting concept, the failure rate function can be updated if necessary.

4.6 Limitations of the proposed formulas

Proposed formulas of PFD_{avg}/PFH calculation have some limitations in application:

1. One channel-one component. The case study considered in this Chapter has a redundancy architecture 1oo2 with two identical channels. Each channel contains only one component affected by wear. Therefore, the failure rate function can be easily obtained if Weibull parameters of the degrading component are known. However the situation becomes more complicated if there are two or more components in one channel. In this case it is required to derive a cumulative distribution function of failures for one channel that can be complicated. Even if the CDF for the channel can be obtained, this is already not necessarily a Weibull distribution. The proposed analytical formulas can be used in case of several components in one channel. However it is possible only if Weibull parameters were obtained for the whole channel, but not for each component of this channel separately. Calculation of PFD_{avg}/PFH also can be conducted by taking into account a failure rate function of a critical degrading component in one channel and relaxation of other components with high reliability.
2. Identical channels. Another limitation of the proposed formulas is identical channels. Therefore calculation of PFD_{avg}/PFH values for heterogeneous redundancy architecture with different channels cannot be performed by using the formulas proposed in this Chapter.

4.7 Conclusions

This Chapter presented new analytical formulas of reliability assessment of redundant M-out-of-N systems with non-constant failure rates. The main results obtained in this Chapter are listed below:

1. Developed formulas for PFD_{avg} calculation showed results that are very close to the results obtained by using the exact method (Δ_{avg}=0.2%). Comparison of obtained simplified formulas of PFH calculation with full formulas also showed a very small difference (Δ_{avg}=0.4%) for all degradation effects in the considered case studies.
2. Contribution from CCFs is significant for calculation of PFD_{avg} and PFH values especially in formulas of prognosis. Developed formulas of PFD_{CCF} and PFH_{CCF} showed increase each test interval.
3. Obtained PFH formulas showed the same results for α=1 as formulas for the exponential case.
4. Numerical results presented in Section 4.5 demonstrated the necessity of using a failure rate function for systems with strong degradation in the wear out region.
5. Derivation of analytical formulas for PFD_{avg}/PFH calculation for redundant safety systems with non-constant failure rates, presented in this Chapter, answers to the third research question: "*Which analytical formulas can be developed for PFD_{avg}/PFH calculation of redundant safety systems with non-constant failure rates?*".

Limitations of the proposed formulas, discussed in Section 4.6, require development of the new method that could cope with these limitations. Such method will be presented in Chapter 5.

References

Aschenbrenner, S. (2004) FMEDA and Proven-in-use assessment. Exida Project: Inductive NAMUR sensors. Report No.: P+F 03/11-10 R015, Germany.

Barringer & Associates, Inc. (2010) *Weibull Database.* Available at: http://www.barringer1.com/wdbase.htm (Accessed 1 May 2016).

Bertsche B. (2008) *Reliability in automotive and mechanical engineering*. Germany: Springer-Verlag Berlin Heidelberg.

Chebila, M. and Innal, F. (2015) Generalized analytical expressions for safety instrumented systems' performance measures: PFD_{avg} and PFH. *Journal of Loss Prevention in the Process Industries*, 34, pp.167-176.

Chudoba, J. (2011) Modelling of dynamical dependability by using stochastic processes, *European Safety and reliability conference (ESREL)*, Troyes, France. 18-22 September 2011, London: Taylor & Francis Group, pp. 2045–2049.

Dersin, P., Peronne, A., Arroum, C. Selecting test and maintenance strategies to achieve availability target with lowest life-cycle cost. *Reliability and Maintainability Symposium*, Las Vegas, NV. 28-31 January 2008, IEEE, pp. 301-306.

Hauge, S. and Lundteigen, M.A. (2008) Guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase. SINTEF report A8788, Trondheim, Norway.

Hauge, S., Habrekke, S., Lundteigen, M.A. (2010) *Reliability Prediction Method For Safety Instrumented Systems – PDS Example collection.* SINTEF report A17956, Trondheim, Norway.

International Electrotechnical Commission (IEC) (2005) IEC 62061. Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems.

International Electrotechnical Commission (IEC) (2010) IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1-7.

International Organization for Standardization (ISO) (2015) ISO 13849-1. Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design.

Jigar, A.A. (2013) *Quantification of Reliability Performance: Analysis Methods for Safety Instrumented System*. Master thesis, NTNU, Trondheim, Norway.

Jin, H., Lundteigen, M.A., Rausand, M. (2013) New PFH-formulas for k-out-of-n: F-systems. *Reliability Engineering and System Safety*, 111, pp.112–118.

Kumar, R. and Jackson, A. Accurate reliability modeling using Markov analysis with non-constant hazard rates. *IEEE Aerospace conference*, Big Sky, MT. 7-14 March 2009, IEEE, pp. 1-7.

Pozsgai, P., Neher, W., Bertsche, B. (2002) Models to Consider Dependence in Reliability Calculation for Systems Consisting of Mechanical Components. In *Proc. of MMR 2002*, Trondheim, Norway, 17-20June, 2002, pp. 539-542.

Rausand, M. (2014) *Reliability of Safety-Critical Systems Theory and Applications*. Hoboken, NJ: John Wiley & Sons, Inc.

Rausand, M. and Høyland, A. (2004) System reliability theory; models, statistical methods, and applications. 2nd edn. Hoboken, NJ: Wiley.

Rogova E and Lodewijks G. (2015) Braking system redundancy requirements for moving walks. *Reliability Engineering and System Safety*, 133, pp.203–211.

Rogova, E., Lodewijks, G., Lundteigen, M.A. (2015) Analytical formulas of PFD calculations for systems with non-constant failure rates. In: *European Safety and* *reliability conference (ESREL)*, Zurich, Switzerland. 7-10 September 2015, London: Taylor & Francis Group, pp.1699–1707.

Rogova E., Lodewijks G., Lundteigen M.A. (2017) Analytical formulas of PFD and PFH calculation for systems with non-constant failure rates. *Proc IMechE Part O: Journal of Risk and Reliability*, special issue, pp.1–10.

Santos, F.P., Teixeira, A.P., Guedes Soares, C. (2014) An age-based preventive maintenance for offshore wind turbines, *European Safety and reliability conference (ESREL)*, Wroclaw, Poland. 14-18 September 2014, London: Taylor & Francis Group, pp. 1147–1155.

Siemens (2014) Overview of Safety-Related Parameters for Siemens Components in Accordance with ISO 13849-1 and IEC 62061. Version 0.56, Nürnberg, Germany.

Sung B.-J. (2012) A Design Method and Reliability Assessment of High Speed Solenoid Actuator, *Journal of International Council on Electrical Engineering,* 2(1), pp.110-118.

Vatn, J. (2006) Procedures for updating test intervals based on experience data. *The 30th ESReDa Seminar*, Trondheim, Norway, 7-8 June 2006.

Chapter 5

Window-based Markov method[*]

Application of an M-out-of-N redundancy architecture is a well-known measure for improving the reliability of safety systems. As was shown in Chapter 2, most scientific papers addressing the reliability assessment of such systems consider a conventional homogeneous M-out-of-N redundancy architecture that is performed for identical channels. Analytical formulas of PFD_{avg} and PFH calculation for such architecture were developed in Chapter 4. However, often in practice M-out-of-N redundancy architecture does not have identical channels. Reliability assessment of such heterogeneous systems (electrical/electronic and mechanical) with non-identical channels and a combination of constant and non-constant failure rates is considered in this Chapter. Such type of M-out-of-N redundancy architecture is introduced in this research as "asymmetrical redundancy". It can be used for enhancing the reliability of old mechanical systems or for reducing mutual influence of channels and increase of diagnostic coverage. This Chapter also presents a new "window-based Markov method" for PFD_{avg} and PFH calculation for systems with an asymmetrical redundancy architecture, and compares the results with the results obtained by using the steady-state semi-Markov method, and Monte Carlo simulation. The applicability of the developed window-based Markov method is demonstrated in a case study.

This Chapter is organized as follows. Section 5.1 considers asymmetrical redundancy as a type of heterogeneous redundancy architecture, and common cause failures in systems with asymmetrical redundancy architecture. Section 5.2 demonstrates the principles of calculation of PFD_{avg} and PFH values for systems with asymmetrical redundancy architecture by using the new window-

[*] This chapter is based on E. Rogova, G. Lodewijks, E. Calixto, (2017)

based Markov method. A case study is described in Section 5.3 with comparison of numerical results by using the window-based Markov and the steady-state semi-Markov methods. The results are also compared with the results obtained by Monte Carlo simulation in Section 5.4. Section 5.5 concludes.

5.1 Asymmetrical Redundancy

Redundancy allocation is used in many safety systems as one of the effective ways to improve their reliability: “Redundancy is commonly used in system design to enhance systems reliability, especially when it is difficult to increase component reliability itself” (Kuo and Zhu, 2012) There are many definitions of redundancy. For instance, standard IEC 61508 describes this as an existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information (IEC 61508-4, 2010). Rausand states that redundancy implies having two or more items, such that if one item fails, the system can continue to function by using the other item(s) (Rausand, 2014).

Systems with an M-out-of-N redundancy architecture have a wide range of applications in different engineering fields. “The capabilities of M-out-of-N redundancy make it an important tool for failure prevention. Sometimes components are deliberately subdivided in order to permit M-out-of-N redundancy to be applied” (Hecht, 2004). The definition of M-out-of-N redundancy architecture is given by Rausand and Høyland: “a system that is functioning if and only if at least M of the N components are functioning is called a M-out-of-N structure (MooN)” (Rausand and Hoyland, 2004). The definition of an M-out-of-N architecture prescribes that N channels are identical. In practice very often channels in M-out-of-N architecture are not totally identical and sometimes they are very different: heterogeneous. Heterogeneous redundancy is defined as mixing of different types of components (Sharma et al., 2011). Such type of heterogeneous M-out-of-N redundancy architecture is considered in the literature by a few researchers. Boddu and Xing consider redundancy allocation for M-out-of-N architecture with mixed spare types (Boddu and Xing, 2012). Li and Ding conducted research about optimal allocation policy of active redundancies to M-out-of-N systems with heterogeneous components (Li and Ding, 2010). The question of reliability estimation of heterogeneous multi-state series-parallel systems was investigated by Sharma et al. (2011), Wang and Li (2012). However, these papers are mainly focused on existing heuristic algorithms and difficulties related to combinatorial optimization and do not aim at a practical calculation of system reliability in the concept of functional safety. This Chapter presents derivation of $\mathrm{PFD}_{\mathrm{avg}}$ (Average Probability of Failure on Demand) and PFH (Average Frequency of Dangerous Failures) values for heterogeneous M-out-of-N systems with non-identical channels (electronic/electrical and mechanical) and combination of constant and non-constant failure rates by using a new window-based Markov method.

The failure rates of many electronic/electrical components can be considered as approximately constant. However, often a non-constant failure rate is the only valid option for the reliability analysis of mechanical components with degradation over time, when the process cannot be approximated by an exponential law and the test interval is quite large. Indeed, for low-demand safety systems the proof-test interval is usually in the order of 6 months to 2-3 years (Rausand and Hoyland, 2004). This test interval can be too large for an approximation by a constant failure rate in case of degrading systems.

As was shown in Chapter 2, some channels of a heterogeneous M-out-of-N redundancy architecture have constant failure rates and others – non-constant failure rates. Such architecture may be used, for example, in old mechanical safety systems when, instead of its full replacement, a redundancy can be introduced by adding the appropriate electrical/electronic components into the system. Such hardware diversity can also be used in safety systems for reducing common cause failures and for increase of the diagnostic coverage (DC) which is “fraction of dangerous failures detected by automatic on-line diagnostic tests” (IEC 61508-4, 2010). In these cases channels with mechanical components and channels with electrical/electronic components perform the same safety function. To identify such safety systems, a new term of heterogeneous redundancy is introduced here. *Asymmetrical redundancy* is a type of M-out-of-N redundancy allocation with non-identical channels (mechanical/electrical/electronic) that perform the same safety function, but are based on a different physical principle and failure rates (constant and non-constant). The term asymmetrical redundancy is used in network theory, chip technologies (Osewold et al., 2014), control systems (Essame et al., 1999), but it has not been used in reliability theory. There is a research about asymmetrical failure modes in reliability of digital systems (Meisel and Schaeffer, 1969), which however does not consider asymmetrical redundancy.

5.1.1 Types of asymmetrical redundancy architecture

There are several possible configurations of asymmetrical redundancy. Figure 5.1 shows three simple cases of asymmetrical redundancy with two (a) and three (b,c) non-identical channels. Case (a) presents one channel with a mechanical component and non-constant failure rate (z(t)) and another channel with an electrical/electronic component and approximately constant failure rate (λ). This for example can be a safety system of an elevator with a mechanical system and an infrared system which detect objects between the elevator doors.

Case (c) in Figure 5.1 can be used for a system of level control. If two mechanical level sensors (z_1(t) and z_2(t)) have been already installed, the third electronic radar sensor (λ) can be installed as an additional third channel (for implementation of voting logics 2oo3 for example) etc.

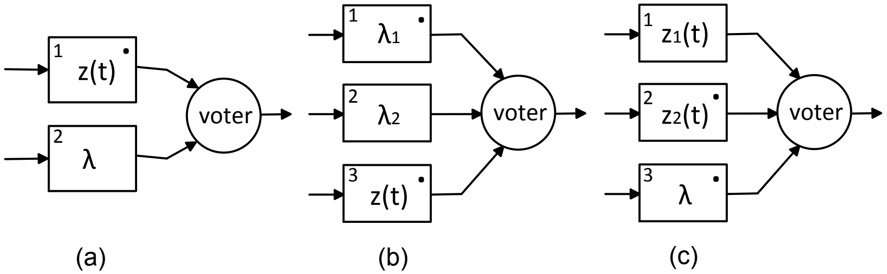


Figure 5.1: Different configurations of asymmetrical redundancy architecture.

A special notation for asymmetrical redundancy is proposed here for those cases, when it is important to know concrete channels from which the signal is obtained (see tokens in Figure 5.1). Thereby M_i-out-of-N, where M – is the number of functioning channels, $i(\overline{1,M})$- specific numbers of functioning channels, and N – is the number of all channels. Cases (b) and (c) with three non-identical channels can be denoted: $2_{1,3}oo3$ and $2_{2,3}oo3$ respectively. For $2_{1,3}oo3$ architecture it may be important to have signals from a mechanical channel z(t) and from an electrical/electronic channel λ_1. Sometimes signals from mechanical channels must be compared with signals from electronic/electrical channels. For example, such comparison is required on the stage of system debugging and for an increase of diagnostic coverage. For $2_{2,3}oo3$ architecture the existence of only two signals z_1(t) and z_2(t) may be unacceptable because both channels (1 and 2) are mechanical and there is no possibility to compare them with a signal from an electronic system. However, such designation and marking with tokens of specific channels is not always required. Asymmetrical redundancy can use common notation MooN if there are no any preferences to get information from specific channels (mechanical or electronic/electrical).

There are many possible configurations of asymmetrical redundancy architecture, and they all depend on a concrete safety system and required functions that have to be performed. However reliability assessment of such systems does not have differences with reliability assessment of non-marked M-out-of-N redundancy architecture. The difference can be found only in the value of a diagnostic coverage and in a control system, because a lack of signals or incorrect values obtained from marked channels will be sent and processed in PLC for taking a decision about further functionality of a system.

5.1.2 CCF in systems with asymmetrical redundancy architecture

The standard IEC 61511 defines a CCF (common cause failure) as a failure which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to a system failure (IEC 61511-1, 2003). IEC 61508 and IEC 61511 classify these failures mainly as systematic failures, i.e. failures which are intrinsic to the design of a redundant system. Indeed, the design of redundant systems needs to take into account possible mutual influence of channels, because such common failures can significantly reduce the reliability of a system. In case of neglecting of CCF impact to reliability calculation, obtained results may be too optimistic. The simplified Euler diagram in Figure 5.2 shows CCFs as an intersection of failures of mechanical M and electronic E channels.

One of the most convenient and wide-spread models for numerical calculation of CCF is a β-factor model. Most researchers and functional safety standards (IEC 61508, IEC 61511) consider constant β values for the characteristic of CCF even for degrading redundant systems with identical channels and the same Weibull shape parameters (Pozsgai et al. 2002).

Sometimes the beta factor is changing (*β(t)≠const*) together with the increase of the failure rate in degrading channels. This issue is considered by (Pozsgai et al., 2002). However in this thesis we do not consider this phenomenon, and assume that *β*-factor is constant.

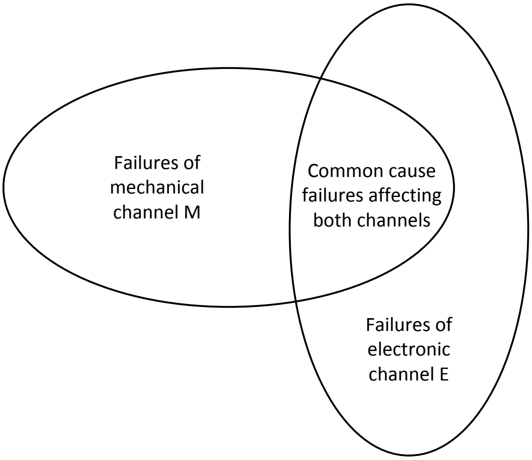

Failures of mechanical channel M
Common cause failures affecting both channels
Failures of electronic channel E

Figure 5.2: Euler Diagram of CCFs for asymmetrical redundancy architecture with M (mechanical) and E (electronic) channels.

At the same time, asymmetrical redundancy represents a type of hardware diversity in channels. The standard IEC 61508-7 describes hardware diversity as a way to detect and reduce systematic failures, using different types of components with different rates and types of failures in the diverse channels of a safety related system (IEC 61508-7, 2010). This means that *β*-factor is significantly smaller for systems with asymmetrical redundancy that is demonstrated by a checklist provided by IEC 61508-6 (IEC 61508-6, 2010) in Table 5.1:

Table 5.1: Scoring programmable electronics or sensors/final elements (IEC 61508-6, 2010).

Item	Score X_{SF}
Do the devices employ different physical principles for the sensing elements for example, pressure and temperature, vane anemometer and Doppler transducer, etc?	9

where X_{SF} is a corresponding value for the sensors.

The principle of work of such checklists is based on summation of scores in case of a positive answer to the question. The more value of such scores, the less mutual influence of channels and smaller the value of β-factor. The standard IEC 62061 also suggests a checklist for the determination of CCF (Table 5.2). Both checklists (IEC 61508 and IEC 62061) show high scores for diverse channels. Maximum value of scores in these checklists is 10.

Table 5.2: Criteria for estimation of CCF (IEC 62061, 2005).

Item	Score
Does the subsystem employ elements that use different physical principles (e.g. sensing elements at a guard door that use mechanical and magnetic sensing techniques)?	10

Therefore, in general, CCFs can increase in systems with non-constant failure rates due to the degradation of equipment in channels and increase of their mutual influence. However, asymmetrical redundancy uses a principle of hardware diversity, and work of channels is based on different physical principles. Therefore, for such systems the values of β-factors are significantly reduced that means increase of reliability.

5.2 New Window-Based Markov Method

There are two issues in the reliability assessment of systems with asymmetrical redundancy. The first issue is the non-identical channels. The second issue is the non-constant failure rates. The latter issue is related to degrading components in channels that cause the increase of failure rate. There are a few methods of reliability assessment for solving the first issue (reliability block diagram, Markov methods presented in Chapter 2), and there are also a few methods for solving the second issue (for example, the analytical formulas developed in Chapter 4). However, there are no practical methods capable of coping with both them simultaneously.

The combination of the described issues (non-constant failure rates and non-identical channels), drawbacks of the existing methods, and limitations of the semi-Markov method lead to the development of the practical method that can be applied to cover both of these issues and will be easy to use in practice.

Despite the inability to apply the Markov method to the reliability assessment of systems with degradation, the Markov method can be applied discretely. This Section presents a new "window-based Markov method" for reliability assessment of systems with asymmetrical redundancy architecture. The method is based on the discretization of the failure rate function, and allows to apply the Markov model to each discrete interval of the failure rate function.

In case of discretization of the failure rate function, it has to be divided into discrete regions (windows). Inside each window the failure rate is approximately constant, and the conventional Markov method can be applied. Markov process has to be stopped on a special announced discretization condition at the end of a discrete region: for example, degradation of a system in *p%* or increase of a failure rate in *n* times or other possible conditions. After the end of the first discrete region, the process "jumps" to the second discrete region (window), when system behavior is assumed to be approximately constant again etc. For the next window the failure rate value should be updated together with update of the initial state probabilities. The number of windows is based on the rule: during one discrete region failure rate is considered as approximately constant with a corresponding error (Δ,%) which is estimated in Section 5.4. This error can be different for different systems. Therefore, the number of windows depends on the required accuracy. However in general the more discrete regions are selected, the more accurate and realistic result will be obtained. Large number of discrete regions brings the discretization to the real continuous process. The question of accuracy of results obtained by window-based Markov method is considered in Section 5.4. in more details.

The window-based Markov method is demonstrated for an 1-out-of-2 redundancy architecture as one of the "most commonly used SIS (Safety Instrumented Systems) architectures" (Oliveira, 2008). Here 1oo2 redundancy architecture is asymmetrical: one of the channels is electrical/electronic (E) with constant failure rate λ and the corresponding exponential CDF, and another one is mechanical (M) with non-constant failure rate z(t) and the corresponding Weibull CDF (Figure 5.1a). The diagram of states for the window-based Markov method is presented in Figure 5.3.

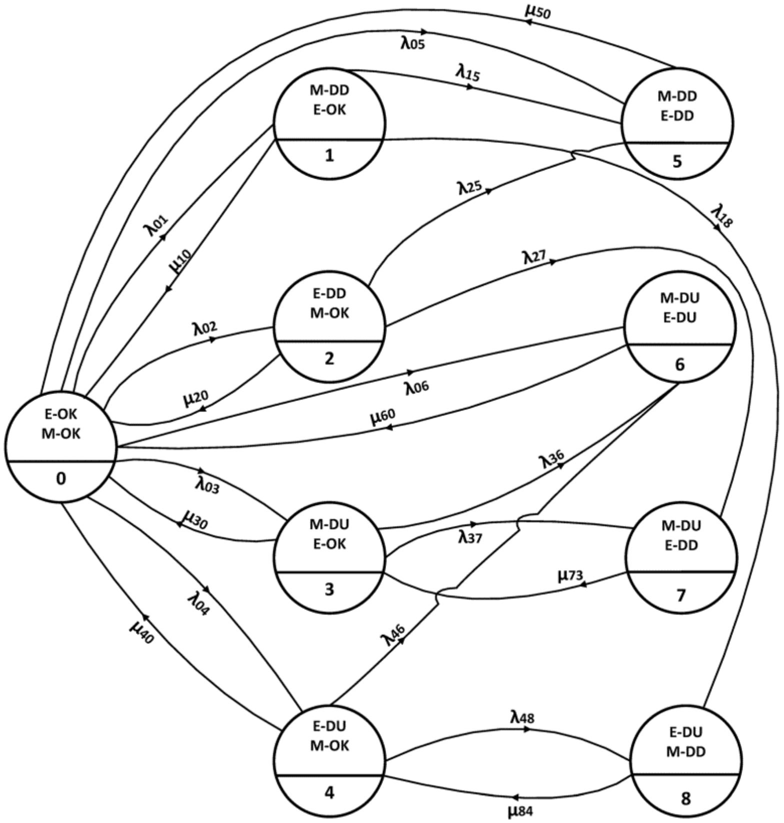


Figure 5.3: State diagram for the window-based Markov method.

There are two possible failures: dangerous detected (DD) and dangerous undetected (DU). For example, state 2 means that channel E has a DD failure, but channel M is able to function (OK). State 7 describes a system state when both channels are down: channel E has a DD failure, and channel M has a DU failure etc. Thereby Figure 5.3 demonstrates that the system is able to perform a required function in states 0-4, and the system fails in states 5-8.

The state diagram has transitions that are described by failure- and repair rates like in a conventional Markov method. By using this diagram, the Markov state equations can be composed. Solving these equations gives the state probabilities $P_j(t), j = \overline{0,8}$ for each discrete region. For this case study there are 9 probabilities for each window (discrete region of the failure rate function).

The most used format of state equations of the Markov process can be found in (Rausand and Hoyland, 2004):

$$P(t)\cdot\mathbb{A}=\dot{P}(t) \tag{5.1}$$

where $\mathbb{A}$ – is the transition rate matrix of the Markov process.

And the corresponding matrix form (Rausand and Hoyland, 2004):

$$[P_0(t),\dots,P_r(t)]\cdot\begin{pmatrix}a_{00} & a_{01} & \dots & a_{0r}\\ a_{10} & a_{11} & \dots & a_{1r}\\ \vdots & \vdots & \ddots & \vdots\\ a_{r0} & a_{r1} & \dots & a_{rr}\end{pmatrix}=[\dot{P}_0(t),\dots,\dot{P}_r(t)] \tag{5.2}$$

Another format of presentation of state equations is used here. It is a transpose form of Equation 5.2:

$$\mathbb{A}^T\cdot P(t)^T=\dot{P}(t)^T \tag{5.3}$$

Therefore the matrix form is:

$$\begin{pmatrix}a_{00} & a_{10} & \dots & a_{r0}\\ a_{01} & a_{11} & \dots & a_{r1}\\ \vdots & \vdots & \ddots & \vdots\\ a_{0r} & a_{1r} & \dots & a_{rr}\end{pmatrix}\cdot\begin{bmatrix}P_0(t)\\ P_1(t)\\ \vdots\\ P_r(t)\end{bmatrix}=\begin{bmatrix}\dot{P}_0(t)\\ \dot{P}_1(t)\\ \vdots\\ \dot{P}_r(t)\end{bmatrix} \tag{5.4}$$

It is important to note that the sum of the coefficients in each column of matrix $\mathbb{A}$ in Equation 5.4 should be equal to 0. Another important condition also has to be taken into account:

$$\textstyle\sum_{j=1}^{r}P_j(t)=1 \tag{5.5}$$

Matrix form described by Equation 5.4 also can be presented by a system of Kolmogorov differential equations. The system of differential equations for the considered redundancy architecture can be written as:

$$\begin{cases}\dot{P}_0(t)=\mu_{40}P_4+\mu_{30}P_3+\mu_{60}P_6+\mu_{20}P_2+\mu_{10}P_1+\mu_{50}P_5-P_0(\lambda_{04}+\lambda_{03}+\lambda_{06}+\lambda_{02}+\lambda_{01}+\lambda_{05})\\ \dot{P}_1(t)=\lambda_{01}P_0-P_1(\mu_{10}+\lambda_{15}+\lambda_{18})\\ \dot{P}_2(t)=\lambda_{02}P_0-P_2(\mu_{20}+\lambda_{25}+\lambda_{27})\\ \dot{P}_3(t)=\lambda_{03}P_0+\mu_{73}P_7-P_3(\mu_{30}+\lambda_{37}+\lambda_{36})\\ \dot{P}_4(t)=\lambda_{04}P_0+\mu_{84}P_8-P_4(\mu_{40}+\lambda_{48}+\lambda_{46})\\ \dot{P}_5(t)=\lambda_{15}P_1+\lambda_{25}P_2+\lambda_{05}P_0-\mu_{50}P_5\\ \dot{P}_6(t)=\lambda_{06}P_0+\lambda_{36}P_3+\lambda_{46}P_4-\mu_{60}P_6\\ \dot{P}_7(t)=\lambda_{27}P_2+\lambda_{37}P_3-\mu_{73}P_7\\ \dot{P}_8(t)=\lambda_{48}P_4+\lambda_{18}P_1-\mu_{84}P_8\end{cases} \tag{5.6}$$

The rules of obtaining Equation 5.6 are not explained here. They can be found in books of Rausand and Høyland (2004), Ross (1996).

The matrix $\mathbb{A}$ for the matrix form of Equation 5.4 can be composed based on a system of Equation 5.6. The matrix $\mathbb{A}$ is demonstrated in Equation 5.7:

$$\begin{vmatrix}
-\lambda_{01}-\lambda_{02}-\lambda_{03}-\lambda_{04}-\lambda_{05}-\lambda_{06} & \mu_{10} & \mu_{20} & \mu_{30} & \mu_{40} & \mu_{50} & \mu_{60} & 0 & 0 \\
\lambda_{01} & -\mu_{10}-\lambda_{15}-\lambda_{18} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\lambda_{02} & 0 & -\mu_{20}-\lambda_{25}-\lambda_{27} & 0 & 0 & 0 & 0 & 0 & 0 \\
\lambda_{03} & 0 & 0 & -\mu_{30}-\lambda_{37}-\lambda_{36} & 0 & 0 & 0 & \mu_{73} & 0 \\
\lambda_{04} & 0 & 0 & 0 & -\mu_{40}-\lambda_{48}-\lambda_{46} & 0 & 0 & 0 & \mu_{84} \\
\lambda_{05} & \lambda_{15} & \lambda_{25} & 0 & 0 & -\mu_{50} & 0 & 0 & 0 \\
\lambda_{06} & 0 & 0 & \lambda_{36} & \lambda_{46} & 0 & -\mu_{60} & 0 & 0 \\
0 & 0 & \lambda_{27} & \lambda_{37} & 0 & 0 & 0 & -\mu_{73} & 0 \\
0 & \lambda_{18} & 0 & 0 & \lambda_{48} & 0 & 0 & 0 & -\mu_{84}
\end{vmatrix} \quad (5.7)$$

where transition rates are described in Table 5.3:

Table 5.3: Transition rates for the window-based Markov method for the *k-th* discrete. region.

λ_{ij}	Expression	λ_{ij}, μ_{ij}	Expression
λ_{01}	$(1-\beta_D)z_M^{DD}(\mathrm{t}_k)$	λ_{37}	λ_E^{DD}
λ_{02}	$(1-\beta_D)\lambda_E^{DD}$	λ_{46}	$z_M^{DU}(\mathrm{t}_k)$
λ_{03}	$(1-\beta)z_M^{DU}(\mathrm{t}_k)$	λ_{48}	$z_M^{DD}(\mathrm{t}_k)$
λ_{04}	$(1-\beta)\lambda_E^{DU}$	μ_{50}	μ^{2DD}
λ_{05}	$\beta_D \cdot \sqrt{\lambda_E^{DD} \cdot z_M^{DD}(\mathrm{t}_k)}$	μ_{60}	μ^{2DU}
λ_{06}	$\beta \cdot \sqrt{\lambda_E^{DU} \cdot z_M^{DU}(\mathrm{t}_k)}$	μ_{73}	μ_E^{DD}
λ_{15}	λ_E^{DD}	μ_{84}	μ_M^{DD}
λ_{18}	λ_E^{DU}	μ_{10}	μ_M^{DD}
λ_{25}	$z_M^{DD}(\mathrm{t}_k)$	μ_{20}	μ_E^{DD}
λ_{27}	$z_M^{DU}(\mathrm{t}_k)$	μ_{30}	μ_M^{DU}
λ_{36}	λ_E^{DU}	μ_{40}	μ_E^{DU}

Failure rates λ_{01}, λ_{02}, λ_{03}, λ_{04} present independent failures of channels. Failure rates λ_{05}, λ_{06} present dependent failures, and they are considered as common cause failures. These failure rates correspond to the situation when both channels have DD failures (λ_{05}) or DU failures (λ_{06}) simultaneously: if $\lambda_E^{DD} = z_M^{DD}(\mathrm{t}) = \lambda^{DD}$ or $\lambda_E^{DU} = z_M^{DU}(\mathrm{t}) = \lambda^{DU}$, then $\lambda_{05} = \beta_D \cdot \lambda^{DD}$ and $\lambda_{06} = \beta \cdot$

λ^{DU}. CCFs are modeled by a β-factor model where β is applied for DU failures, and β_D – for DD failures. Formulas presented in Table 5.3 for λ_{05} and λ_{06} also can be found in Hildebrandt, 2007. Failure rates λ_{15}, λ_{18}, λ_{25}, λ_{27}, λ_{36}, λ_{37}, λ_{46}, and λ_{48} include only failure rates of one of two channels because the other one is assumed to be in a failure state.

Repair distribution is assumed to be exponential for both channels. Repair rates μ_{50}, μ_{60}, μ_{73}, μ_{84}, μ_{10}, μ_{20}, μ_{30}, and μ_{40} are presented in Equations 5.8-5.11 (Rausand, 2014):

$$\mu_E^{DU} = \mu_M^{DU} = \frac{1}{{}^{\tau}/_{2}+MRT} \quad (5.8)$$

$$\mu_E^{DD} = \mu_M^{DD} = \frac{1}{MTTR} \quad (5.9)$$

$$\mu^{2DD} = \frac{1}{2MTTR} \quad (5.10)$$

$$\mu^{2DU} = \frac{1}{{}^{\tau}/_{3}+MRT} \quad (5.11)$$

where MTTR – is mean time to restoration (hour), MRT is mean repair time (hour), and τ is test interval.

The system of Kolmogorov equations (Equation 5.6) can be solved by using numerical methods like Runge-Kutta method (4-5 orders). It is important to remember that initial state probabilities for the first window are: [1 0 0 0 0 0 0 0 0] (where P_0=1). But initial probabilities for the second and further windows are the results of the previous windows (Table 5.4). Besides changing the initial probabilities each window, it is necessary to change the discrete values of the failure rates. This procedure will be shown numerically in Section 5.3.2. The final values of the state probabilities for the continuous process which was discretized, are presented by state probabilities in the last discrete region (Window N).

PFD_{avg} value for this method is calculated as:

$$PFD_{avg} = P_5^N(t_N)+P_6^N(t_N) + P_7^N(t_N) + P_8^N(t_N) \quad (5.12)$$

Safety availability of a system can be determined as:

$$A = P_0^N(t_N) + P_1^N(t_N) + P_2^N(t_N) + P_3^N(t_N) + P_4^N(t_N) \quad (5.13)$$

Table 5.4: Initial, final probabilities and discrete failure rates for each window of the window-based Markov method.

	Window 1		Window 2		Window N	
State probabilities	Initial	Final	Initial	Final	Initial	Final
	1	$P_0^1(t_1)$	$P_0^1(t_1)$	$P_0^2(t_2)$	$P_0^{N-1}(t_{N-1})$	$P_0^N(t_N)$
	0	$P_1^1(t_1)$	$P_1^1(t_1)$	$P_1^2(t_2)$	$P_1^{N-1}(t_{N-1})$	$P_1^N(t_N)$
	0	$P_2^1(t_1)$	$P_2^1(t_1)$	$P_2^2(t_2)$	$P_2^{N-1}(t_{N-1})$	$P_2^N(t_N)$
	0	$P_3^1(t_1)$	$P_3^1(t_1)$	$P_3^2(t_2)$	$P_3^{N-1}(t_{N-1})$	$P_3^N(t_N)$
	0	$P_4^1(t_1)$	$P_4^1(t_1)$	$P_4^2(t_2)$	$P_4^{N-1}(t_{N-1})$	$P_4^N(t_N)$
	0	$P_5^1(t_1)$	$P_5^1(t_1)$	$P_5^2(t_2)$	$P_5^{N-1}(t_{N-1})$	$P_5^N(t_N)$
	0	$P_6^1(t_1)$	$P_6^1(t_1)$	$P_6^2(t_2)$	$P_6^{N-1}(t_{N-1})$	$P_6^N(t_N)$
	0	$P_7^1(t_1)$	$P_7^1(t_1)$	$P_7^2(t_2)$	$P_7^{N-1}(t_{N-1})$	$P_7^N(t_N)$
	0	$P_8^1(t_1)$	$P_8^1(t_1)$	$P_8^2(t_2)$	$P_8^{N-1}(t_{N-1})$	$P_8^N(t_N)$
Discrete	$z_{DU}^M(t_1)$		$z_{DU}^M(t_2)$		$z_{DU}^M(t_N)$	
failure rates	$z_{DD}^M(t_1)$		$z_{DD}^M(t_2)$		$z_{DD}^M(t_N)$	

The following transitions give a dangerous failure of the voted group: 0→5, 0→6; 1→5, 1→8; 2→5, 2→7; 3→6, 3→7; 4→6, 4→8.

The value of PFH(t_N) at time t_N can therefore be determined as:

$$PFH(t_N) = P_0^N(t_N) \cdot (\lambda_{05} + \lambda_{06}) + P_1^N(t_N) \cdot (\lambda_{15} + \lambda_{18}) + P_2^N(t_N) \cdot (\lambda_{25} + \lambda_{27}) + P_3^N(t_N) \cdot (\lambda_{36} + \lambda_{37}) + P_4^N(t_N) \cdot (\lambda_{46} + \lambda_{48}) \tag{5.14}$$

The window-based Markov method described in this section is applied for an 1oo2 asymmetrical redundancy architecture. As was discussed in Section 5.1.1, there are two possible types of asymmetrical 1oo2 redundancy architecture (1_1oo2 and 1_2oo2) but the selected type of redundancy does not affect to the state diagram and calculations.

It is important to note, that the time of discretization in the window-based Markov method is not necessarily equal for each window. For example, for those intervals, where changes are more intensive, periods of time can be shorter. For those intervals, where changes are not so intensive, periods of time can be larger (within the range of the allowable accuracy). However, the sum of probabilities should be equal to 1 at any period of time for each window. In such a way the correctness of calculations can be easily checked. In addition, the maximum allowed error for the discretization of the failure rate function can be also determined. Thereby simplicity, accuracy, easy check of correctness and applicability to systems with non-constant failure rates are the advantages of this method.

5.3 Case study

In this section the numerical example of calculation of $\mathrm{PFD}_{\mathrm{avg}}$ and PFH values is considered by using the window-based Markov method. This case study was designed to demonstrate:

- The applicability of the window-based Markov method to the calculation of $\mathrm{PFD}_{\mathrm{avg}}$ and PFH values for systems with asymmetrical redundancy;
- Comparison of the results with the results obtained by using the steady-state semi-Markov method.

5.3.1 Description of a system

As an example, a relay system with asymmetrical 1_1oo2 redundancy architecture was chosen. Channel M contains an electro-mechanical relay with degradation over time and non-constant failure rate z(t). Channel E contains an electronic solid-state relay (SSR) with constant failure rate λ. The simplified scheme of redundancy architecture is shown in Figure 5.1a. The marked channel with electro-mechanical relay sends signals to the PLC for processing. These signals should be compared with signals from channel E. In case of incorrect values from channel M it can be decided to switch to the channel E or in case of minor deviations – to follow changes and record them till the critical value that allows getting statistics of degradation and to increase the diagnostic coverage.

Roettjer gives the results of tests for electromechanical relays (Roettjer, 2004). For one of the samples he defines Weibull parameters as: α=1.5, η=400·10^6 cycles. Assuming a case specific number of cycles per hour (600 cycles/hour) and using Equation 2.1, the failure rate function of channel M can be obtained:

$$z_M^D(t) = 2.76 \cdot 10^{-9} \cdot t^{0.5} \tag{5.15}$$

Taking into account a diagnostic coverage DC for failures of channel M:

$$z_M^{DD}(t) = DC \cdot 2.76 \cdot 10^{-9} \cdot t^{0.5} \tag{5.16}$$

$$z_M^{DU}(t) = (1 - DC) \cdot 2.76 \cdot 10^{-9} \cdot t^{0.5} \qquad (5.17)$$

MTBF for electronic SSR is estimated as $19 \cdot 10^6$ hours (IXYS, 2014). Thus, failure rate for the channel E: $\lambda_E^D = 5.26 \cdot 10^{-8}$ (hours^{-1}). Taking into account a diagnostic coverage:

$$\lambda_E^{DD} = DC \cdot 5.26 \cdot 10^{-8} \qquad (5.18)$$

$$\lambda_E^{DU} = (1 - DC) \cdot 5.26 \cdot 10^{-8} \qquad (5.19)$$

DC is chosen as 60% (the minimal one, suggested by IEC 61508-6). Values of common cause failures (for undetected and detected dangerous failures) have been chosen as β=0.1 and β_D=0.05, respectively (middle values suggested by IEC 61508-6). Values of MRT (Mean Repair Time) and MTTR (Mean Time To Restoration) are equal to 8 hours (IEC 61508-6, 2010).The selected test interval τ is 8760 h.

Elementary relays within the scope of the standard IEC 61810-2 are considered as non-repaired items (IEC 61810-2, 2011). Indeed, as follows from Equations 5.15-5.19, reliability of these relays is very high and does not require accounting of repair during one test interval. However in this section repair rates are included for demonstration of all possibilities of the proposed method. Repair rates can be easily set to zero in calculations if necessary.

5.3.2 Numerical calculations by window-based Markov method

The failure rate function in the window-based Markov method has to be discretized as was described in Section 5.2. For the failure rate function in Equation 5.15, 7 discrete regions have been chosen, for each of which a failure rate can be considered as approximately constant. The number of discrete regions of the failure rate function has been chosen taking into account the required accuracy. The period of time t that is considered here is equal to the test interval τ=8760 hours. It has been divided into 7 periods of time: $t_k = n_k^{\frac{1}{\alpha-1}}$, where $n_k = \frac{\lambda_k}{\lambda_0}, k = \overline{1,7}$ and $\lambda_0 = z_M^D(t_0 = 1hour) = 2.76 \cdot 10^{-9}$; $\lambda_{\mathrm{k}} = z_M^D(t_k)$.

For this case study the following discretization has been chosen: it is based on the condition that the value of failure rate for the next discrete region is twice larger than for the previous one. Therefore n_k=[2, 4, 8, 16, 32, 64]. Discrete values of the failure rate function for mechanical channel M (Equations

5.15-5.17) were calculated for these discrete regions and demonstrated in Table 5.5. Numerical values of repair rates were calculated in accordance to Equations 5.8-5.11. If the accuracy has to be increased, the value of n_k can be reduced. The discretization of the failure rate function $z_M^D(t)$ is shown graphically in Figure 5.4. The value of constant failure rate for channel E is also shown for a comparison.

Table 5.5: Numerical values of reliability parameters for the discretized process.

tt_k	$z_M^D(\mathrm{t}_k)$	λ_E^D	DC	$z_M^{DD}(\mathrm{t}_k)$	$z_M^{DU}(\mathrm{t}_k)$	λ_E^{DD}	λ_E^{DU}	β	β_D	μ_E^{DD}, μ_M^{DD}	μ_E^{DU}, μ_M^{DU}	μ^{2DD}	μ^{2DU}
t_1	$5.52\cdot10^{-9}$	$5.26\cdot10^{-8}$	0.6	$3.31\cdot10^{-9}$	$2.21\cdot10^{-9}$	$3.16\cdot10^{-8}$	$2.10\cdot10^{-8}$	0.1	0.05	0.125	$2.28\cdot10^{-4}$	0.0625	$3.42\cdot10^{-4}$
t_2	$1.10\cdot10^{-8}$			$6.62\cdot10^{-9}$	$4.42\cdot10^{-9}$								
t_3	$2.21\cdot10^{-8}$			$1.32\cdot10^{-8}$	$8.83\cdot10^{-9}$								
t_4	$4.42\cdot10^{-8}$			$2.65\cdot10^{-8}$	$1.77\cdot10^{-8}$								
t_5	$8.83\cdot10^{-8}$			$5.30\cdot10^{-8}$	$3.53\cdot10^{-8}$								
t_6	$1.77\cdot10^{-7}$			$1.06\cdot10^{-7}$	$7.07\cdot10^{-8}$								
t_7	$2.58\cdot10^{-7}$			$1.55\cdot10^{-7}$	$1.03\cdot10^{-7}$								

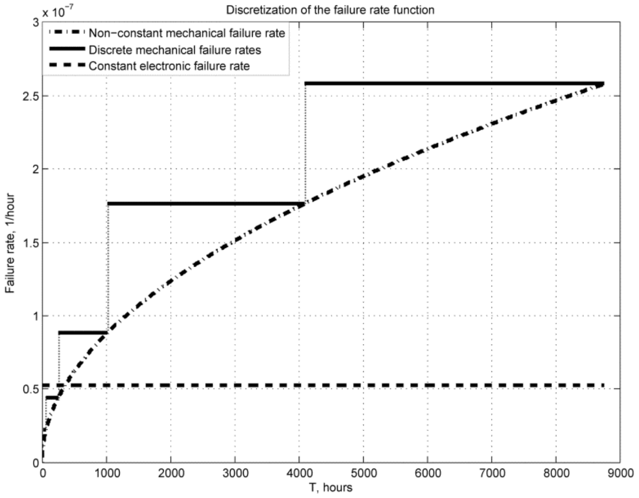


Figure 5.4: Discretization of the failure rate function.

Other discretization models are considered in Section 5.4. A system of Kolmogorov differential equations (Equation 5.6) for the numerical values of Table 5.5 was created and solved 7 times for 7 windows in accordance to the rule described in Section 5.2: calculated state probabilities (P_0-P_8) for the previous discrete region are initial state probabilities for the current discrete region. The correctness of calculations has been checked at the stage of composing a matrix A (Equation 5.7): the sum of elements in a column is equal to 0. The correctness of calculations also has been checked by calculation of a sum of probabilities (Equation 5.5). The values of final probabilities for the last (7th) window and PFD_{avg} values for each window are demonstrated in Table 5.6.

Table 5.6: The numerical results of window-based Markov method.

P_i (7th window)	R (7th window)	PFD_{avg} (for 7 windows)
P0 = 0.9995	0.999986	1st it. $2.0032\cdot10^{-6}$
P1 = $1.1754\cdot10^{-6}$		2nd it. $2.8335\cdot10^{-6}$
P2 = $2.3973\cdot10^{-7}$		3rd it $4.0084\cdot10^{-6}$
P3 = $4.0718\cdot10^{-4}$		4th it. $5.6711\cdot10^{-6}$
P4 = $8.3012\cdot10^{-5}$		5th it. $8.0246\cdot10^{-6}$
P5 = $5.5881\cdot10^{-8}$		6th it. $1.1357\cdot10^{-5}$
P6 = $1.3685\cdot10^{-5}$		7th it. $1.3741\cdot10^{-5}$
P7 = $1.0359\cdot10^{-10}$		
P8 = $1.0663\cdot10^{-10}$		

Figure 5.5 demonstrates an increase of the PFD_{avg} values for the discretized process.

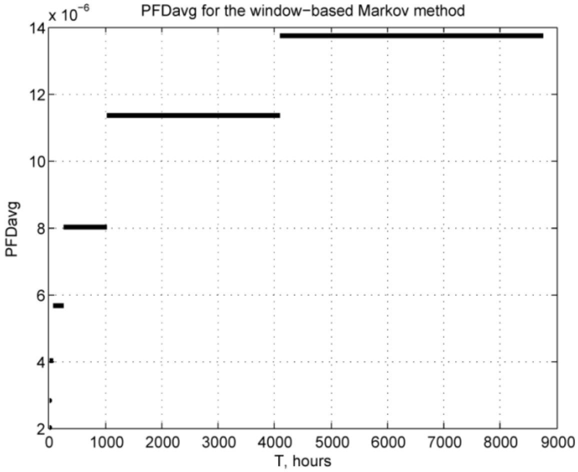


Figure 5.5: Discrete values of PFD_{avg} for the window-based Markov method.

Figures 5.4-5.5 show significant change of failure rate and state probabilities that proves inapplicability of approximation by using a constant failure rate for the whole test interval. It is important to note that the final value of PFD$_{avg}$ is the value for the last discrete period of time.

For systems in a high-demand mode (like the system demonstrated in this section) it is necessary to calculate PFH value in accordance to Equation 5.14. Therefore the PFH value for the last discrete region is:

$$PFH = 8.20 \cdot 10^{-9}$$

Here the calculations for the first proof test interval τ were demonstrated. If after the first test interval no repair or only minimal repair was conducted, update of the failure rate function is not required. The component continues degradation with the same failure rate function. Therefore the window-based Markov method can be applied normally by using the described approach of discretization of the failure rate function. In the case of overhaul, imperfect repair ("not as good as new"), additional number of operating cycles during the proof test, and possible failures that may be induced by proof tests, the failure rate function should be updated. The unified approach of failure rate function update is difficult to develop because the updating procedure should be specified for the component. The procedure of failure rates update is left for future research. However, the window – based Markov method allows to include updated values of failure rate functions. If all required updates of failure rate functions and failure rates were conducted, the principle of calculations of PFD$_{avg}$ / PFH values for the next test intervals is the same as described for the first one.

5.3.3 Numerical calculations by steady-state semi-Markov method and comparison of the results

In this section numerical values of PFD$_{avg}$ and PFH are calculated by using the steady-state semi-Markov method described by Kumar et al. (2013) and compared with the results obtained in Section 5.3.2. Values of steady-state probabilities, reliability and PFD$_{avg}$ values are presented in Table 5.7.

Table 5.7: The numerical results of the steady-state semi-Markov method.

P_i	R	PFD_{avg}
P0 = 0.9972	0.999927	$7.3042 \cdot 10^{-5}$
P1 = $7.6047 \cdot 10^{-6}$		
P2 = $2.3745 \cdot 10^{-7}$		
P3 = 0.0026		
P4 = $8.2126 \cdot 10^{-5}$		
P5 = $2.9741 \cdot 10^{-7}$		
P6 = $7.2744 \cdot 10^{-5}$		
P7 = $6.5853 \cdot 10^{-10}$		
P8 = $6.4563 \cdot 10^{-11}$		

It is interesting to compare the PFD_{avg} value of 1oo2 asymmetrical redundancy architecture with PFD_{avg} for each channel separately. The PFD_{avg} of a single mechanical channel is defined by Equation 5.20 (Rausand and Hoyland, 2004):

$$PFD_{avg}^{1\,channel}(\tau) = MTTR \cdot z_{DD}^{M}(\tau) + z_{DU}^{M}(\tau) \cdot \left(\frac{\tau}{2} + MRT\right) \tag{5.20}$$

In the test interval τ=8760h, the PFD_{avg} for a channel M is equal to $4.55 \cdot 10^{-4}$, and the PFD_{avg} for a channel E is equal to $9.26 \cdot 10^{-5}$. The simplified estimations show that the value of PFD_{avg} for 1oo2 architecture obtained by using the steady-state semi-Markov method ($PFD_{avg}=7.31 \cdot 10^{-5}$) is larger than the PFD_{avg} value obtained by using the window-based Markov method ($PFD_{avg}=1.37 \cdot 10^{-5}$) that proves that steady-state approximation is not applicable for the considered system.

PFH(t) value has to be calculated in case of non-constant failure rates by using Equation 5.14 as follows:

$$PFH(t) = 8.41 \cdot 10^{-10} \cdot t^{0.25} + 6.65 \cdot 10^{-16} \cdot t^{0.5} + 1.39 \cdot 10^{-10} \tag{5.21}$$

Therefore, the average value of PFH can be calculated based on Equation 5.22 (Rausand, 2014):

$$PFH_{avg} = \frac{1}{\tau}\int_0^{\tau} PFH(t)dt \tag{5.22}$$

However it should here be noted that one of the main principles of calculations of the steady-state semi-Markov method is $t \rightarrow \infty$ (Kumar et al., 2013): state probabilities and PFD_{avg} values do not depend on time. The difference in obtained PFD_{avg} values shows that for the considered system the steady-state solution (with $t \to \infty$ and constant state probabilities), cannot be applied. This is also proved by values of state probabilities obtained by the window-based Markov method: they are not constant. For the same reason Equations 5.21-5.22 are not applicable for PFH calculation by using the steady-state semi-Markov method.

5.4 Validation of the window-based Markov method by Monte Carlo Simulation

The validation of the window-based Markov method is presented in this section by comparison of the results obtained by window-based Markov method with the results obtained by Monte Carlo simulation. As a tool for Monte Carlo simulation (MCS), the trial version of BlockSim 10 (Reliasoft) was used. BlockSim provides a possibility to get simulation results for systems modeled as RBD. To use the BlockSim RBD for the validation of the window-based Markov method, the system presented in Section 5.3, was significantly simplified.

As a basis, a system with 1oo2 redundancy architecture is considered here. The influence of CCF is not included (CCF=0), and all failures are considered as dangerous undetected (that means a lack of diagnostics): $\lambda_D = \lambda_{DU}$, $\lambda_{DD} = 0$. There is no explicit separation between DD and DU failure rates in BlockSim. CCF, DD and DU failures can be modelled only by inclusion of additional blocks of RBD in BlockSim. Therefore for simplicity, comparison of window-based Markov and RBD MCS is conducted here only for DU failures.

The Markov state diagram for the system with described conditions contains 4 states (as in Figure 6.11). The validation of obtained results was conducted for both non-repairable and repairable systems. Reliability Block Diagram of 1oo2 system in BlockSym is presented in Figure 5.6.

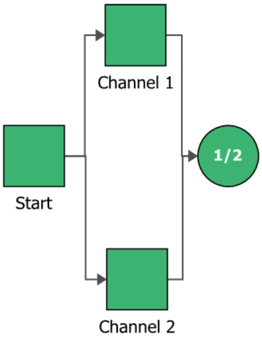


Figure 5.6: RBD for 1oo2 system in BlockSym.

Table 5.8 presents the results obtained for identical degrading channels and for asymmetrical redundancy architecture with different channels and combination of constant and non-constant failure rates for non-repairable systems. EX is exponential distribution, WB is Weibull distribution. RBD MCS results are obtained on the basis of 50000 simulations.

Window-based Markov method allows to calculate values of PFD_{avg}, PFH, availability (A) and reliability (R). RBD MCS in BlockSim allows to calculate values of reliability (R) and availability (A), but does not calculate PFD_{avg} and PFH. Therefore, Table 5.8 presents the values of R (reliability) that were obtained by both – RBD MCS and window-based Markov method. It is important to note that for non-repairable systems availability and reliability are equal. Taking into account that PFD_{avg} is system unavailability, PFD_{avg} can be obtained by using the value of availability as follows:

$$\text{PFD}_{\text{avg}}= 1\text{-A} \qquad (5.23)$$

Discretization of the failure rate function was explained in Section 5.3.1 by using the formula $t_k = n_k^{\frac{1}{\alpha-1}}$, where $n_k = \frac{\lambda_k}{\lambda_0}$. This discretization approach is named Discretization1 (D1) and presented in Table 5.8. However there is another possible way of discretization (Discretization 2 –D2) that is not linked to the increase of the failure rate function during the test interval. This approach is based on dividing the test interval into the equal discrete intervals. The difference between these two approaches is presented graphically in Figure 5.7.

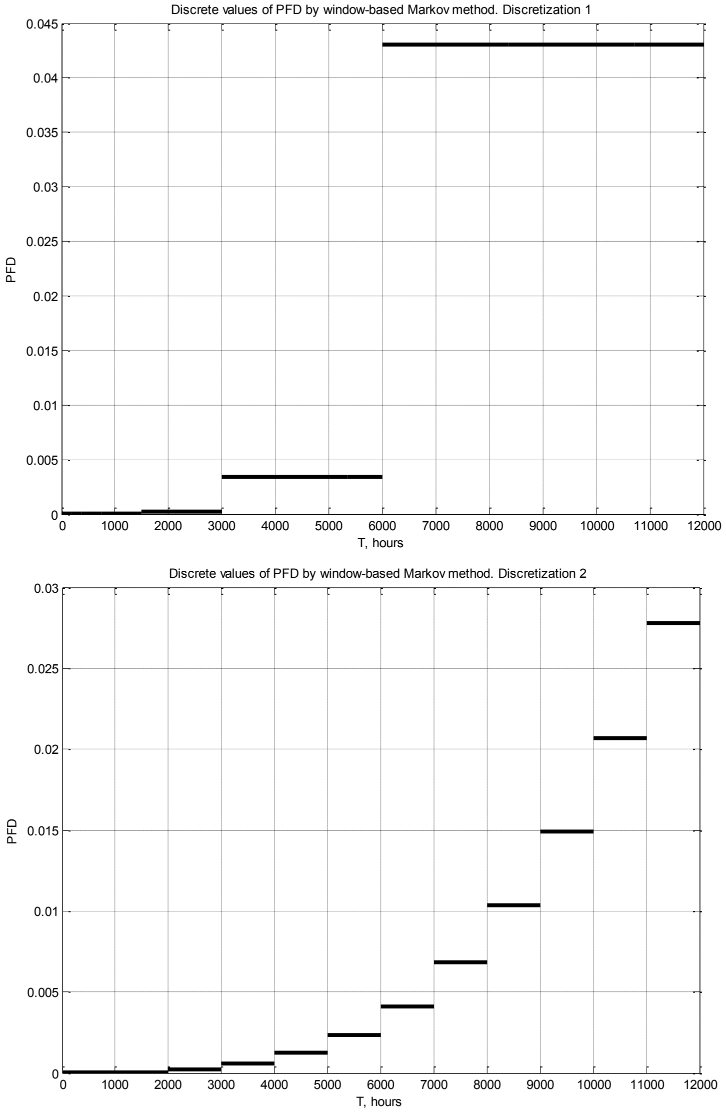


Figure 5.7: Discrete values of PFD obtained by window-based Markov method on the basis of two discretization models.

Figure 5.7 shows discrete values of PFD obtained by window-based Markov method on the basis of two discretization models. The number of discrete intervals presented in Figure 5.7 is the same for both discretization models: it is equal to 12. However in case of Discretization 1 (D1) it is not visually seen because the failure rate function changes mostly at the beginning of the interval, and much less at the end. Discretization 2 (D2) presents uniform discretization with equal time periods that are visually seen in Figure 5.7.

Table 5.8: Comparison of system reliability (R) for non-repairable systems (t=8760h, τ=8760h).

	Non-reparable systems (μ=0)						
	System configuration		**RBD MCS**	**Window-based Markov**		**Δ,%**	
	Channel 1	**Channel 2**		**D1**	**D2**	**Δ_{D1},%**	**Δ_{D2},%**
Identical degrading channels	WB (α=1.5; η=100000)	WB (α=1.5; η=100000)	0.9996	0.9991	0.9993	0.05	0.03
	WB (α=1.5; η=40000)	WB (α=1.5; η=40000)	0.991	0.988	0.990	0.3	0.1
	WB (α=1.5; η=10000)	WB (α=1.5; η=10000)	0.685	0.626	0.665	8.6	2.9
	WB (α=3; η=20000)	WB (α=3; η=20000)	0.994	0.982	0.991	1.2	0.3
	WB (α=3; η=40000)	WB (α=3; η=40000)	0.99994	0.9997	0.9998	0.02	0.01
Different channels (asymmetrical redundancy)	WB (α=1.5; η=10000)	EX (λ=5.26·10^{-5})	0.792	0.774	0.786	2.3	0.8
	WB (α=1.5; η=5000)	EX (λ=5.26·10^{-5})	0.665	0.656	0.663	1.3	0.3
	WB (α=1.5; η=5000)	EX (λ=5.26·10^{-7})	0.9962	0.9957	0.9958	0.05	0.04
	WB (α=1.5; η=10000)	EX (λ=5.26·10^{-7})	0.9975	0.9972	0.9973	0.03	0.02
	WB (α=3; η=10000)	EX (λ=5.26·10^{-5})	0.818	0.747	0.800	8.7	2.2
	WB (α=3; η=5000)	EX (λ=5.26·10^{-7})	0.9958	0.9954	0.9954	0.04	0.04

Results in Table 5.8 obtained by window-based Markov method for non-repairable systems show good correspondence with simulation results. For the considered case studies the mean absolute error in case of discretization 1 (D1) is equal to 2.05%. For discretization 2 (D2) the mean absolute error is equal to 0.61%.

Results obtained for repairable systems are presented in Table 5.9. These results are also obtained for two types of discretization and compared with simulation. It worth to note that due to the lack of diagnostics (there are only undetected failures) the failure can be revealed only during the inspection. In addition, it is assumed that repair of a system is performed “as bad as old” because degradation continues after repair of the component.

The availability (A) values presented in Table 5.9 are obtained for a repairable 1oo2 redundant system with the test interval τ=8760h, and the time of interest (moment of time, when the results should be obtained) t=12000h.

Table 5.9: Comparison of system availability (A) for repairable systems (t=12000h, τ=8760h).

Reparable systems (MRT=8h)						
System configuration		**RBD MCS**	**Window-Based Markov**		**Δ,%**	
Channel 1	**Channel 2**		**D1**	**D2**	**Δ_{D1},%**	**Δ_{D2},%**
WB (α=3; η=2000)	EX ($\lambda=5.26\cdot10^{-5}$)	0.841	0.840	0.854	0.1	1.5
WB (α=3; η=20000)	EX ($\lambda=5.26\cdot10^{-5}$)	0.982	0.957	0.972	2.5	1.0
WB (α=3; η=1000)	EX ($\lambda=10^{-6}$)	0.997	0.997	0.997	0	0
WB (α=1.5; η=5000)	EX ($\lambda=5.26\cdot10^{-5}$)	0.8996	0.858	0.884	4.6	1.7
WB (α=1.5; η=10000)	EX ($\lambda=5.26\cdot10^{-5}$)	0.944	0.903	0.926	4.3	1.9
WB (α=1.5; η=40000)	EX ($\lambda=3\cdot10^{-4}$)	0.963	0.948	0.956	1.6	0.7

Values of availability presented in Table 5.9 show a small difference between simulation results and results obtained by window-based Markov method. For the considered case studies the mean absolute error in case of discretization 1 (D1) is equal to 2.2%. For discretization 2 (D2) the mean absolute error is equal to 1.1%. However as was already shown in Table 5.8 for non-repairable systems, Discretization 2 gives values that are closer to the simulation values. Tables 5.8-5.9 demonstrate that results obtained by window-based Markov method are mainly pessimistic: the values of obtained availability/reliability are lower than that obtained by MCS. This can be explained by pessimistic discretization model: as constant values of the failure rate function, the values at the end (but not at the beginning) of the discrete intervals are taken.

Although the Discretization1 seems a better solution because it is based on the direct connection to the numerical increase of the failure rate function during the test interval, Discretization 2 often gives results that are closer to the results obtained by using Simulation. Therefore if simulation results are considered as “exact” results, Discretization 2 should be chosen. Development of an optimal discretization model for the window-based Markov method is left for future research.

Figure 5.8 shows availability values obtained by window-based Markov method (Discretization 2) and % error for different number of discrete intervals for two case studies: 1) $\alpha=1.5$; $\eta=5000$; $\lambda=5.26\cdot10^{-5}$; $\tau=8760$h without repair; 2) $\alpha=3$; $\eta=20000$; $\lambda=5.26\cdot10^{-5}$; $\tau=12000$h with repair.

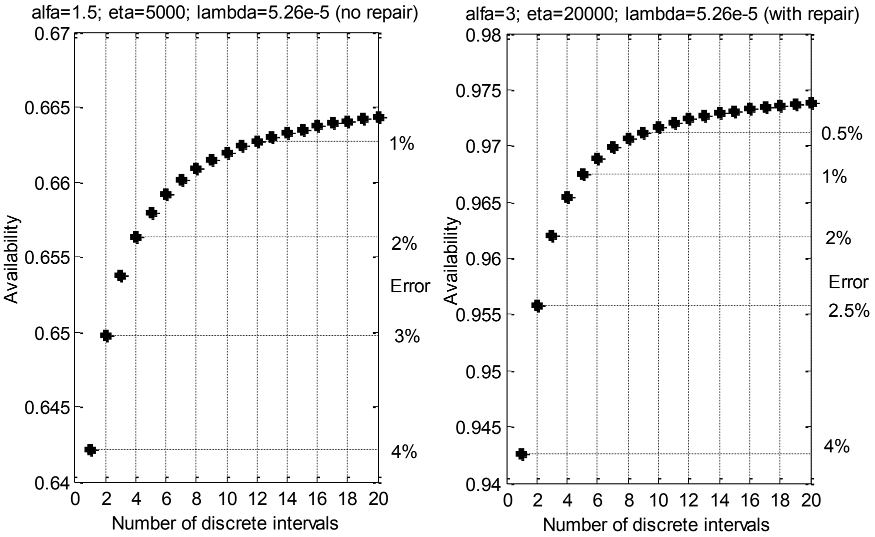


Figure 5.8: Availability values and % error for different numbers of discrete intervals for the case study with and without repair.

Different number of equal discrete intervals was considered. The error around 2 % can be reached even for 3-4 discrete intervals. If 99% is considered as accepted accuracy, for the first system (no repair) in Figure 5.8 it is recommended to apply 12 discrete intervals to reach an accuracy 99%, for the second system (with repair) it is recommended to apply 5 discrete intervals to reach an accuracy 99%. However it is important to note that the number of discrete intervals required to obtain a certain accuracy value is not the same for all redundant systems, it depends on their parameters: Weibull parameters for a degrading channel and the value of failure rate for a channel without degradation.

5.5 Conclusions

Main results obtained in this Chapter are listed as follows:

1. Comparison of the numerical results by the proposed method and by the steady-state semi-Markov method showed inapplicability of the steady-state semi-Markov method for the transient analysis.
2. Comparison of the results obtained by window-based Markov method and results obtained by Monte Carlo simulation showed a very small difference for both non-repairable and repairable systems. The mean absolute error for non-repairable systems is 2% for discretization model D1 and 0.6% for discretization model D2. The mean absolute error for repairable systems is 2.2% for discretization model D1 and 1.1% for discretization model D2 for the considered case studies. Therefore it can be concluded that discretization model D2 showed better results.
3. Increase of number of discrete intervals makes closer the results of window-based Markov method and the results obtained by simulation. In the considered case studies the accuracy 99.4% (D2) for non-repairable and 98.9% (D2) for repairable systems is achieved by using 12 discrete intervals.
4. The application of the proposed window-based Markov method can be limited only in case of large number of channels. In this case the number of system states in window-based Markov method can significantly increase that can create difficulties in calculation.
5. Presented method overcame the limitations of analytical formulas presented in Chapter 4: window-based Markov method can be used if there is more than one component in a channel; it was shown that the method can be used for heterogeneous systems with non-identical channels and combination of constant and non-constant failure rates; the method is independent of the distribution chosen for the failure rate function. Therefore this Chapter gave an answer to the fourth research question: "*How does the developed window-based Markov method overcome the limitations of the developed analytical formulas for reliability assessment?*"

Presented method uses the Weibull distribution for modelling failure rate functions of degrading mechanical components. Weibull shape and scale parameters taken from databases can be used for approximate estimation of failure rate functions. High accuracy of failure rate functions can be achieved only if real degradation data is available. Therefore practical obtaining of failure rate functions and application of the window-based Markov method by using practically obtained failure rate functions will be presented in Chapter 6.

References

Boddu, P. and Xing, L. (2012) 'Redundancy Allocation for k-out-of-n: G Systems with Mixed Spare Types', in *Proc. Reliability and Maintainability Symposium (RAMS)*, (Reno, NV), pp. 1-6.

Essamé, D., Arlat, J., Powell, D. (1999) 'PADRE: A Protocol for Asymmetric Duplex Redundancy', in *Proc. Dependable Computing for Critical Applications 7*, (San Jose, CA, USA).

Hecht, H. (2004) *Systems Reliability and Failure Prevention.* Norwood, MA: Artech House.

Hildebrandt, A. (2007) 'Calculating the "Probability of Failure on Demand" (PFD) of complex structures by means of Markov Models', in *Proc. 4th European Conference on Electrical and Instrumentation Applications in the Petroleum & Chemical Industry*, (Paris, France), pp. 1-5.

International Electrotechnical Commission (IEC) (2004) IEC 61511-1. Functional safety – Safety instrumented systems for the process industry sector. Part 1: Framework, definitions, system, hardware and software requirements.

International Electrotechnical Commission (IEC) (2005) IEC 62061. Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems.

International Electrotechnical Commission (IEC) (2010) IEC 61508-4. Functional safety of electrical/electronic/ programmable electronic safety-related systems. Part 4: Definitions and abbreviations.

International Electrotechnical Commission (IEC) (2010) IEC 61508-7. Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures.

International Electrotechnical Commission (IEC) (2010) IEC 61508-6. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3.

International Electrotechnical Commission (IEC) (2011). IEC 61810-2. Electromechanical elementary relays - Part 2: Reliability.

IXYS Integrated Circuits Division. (2014) Advantages of Solid-State Relays Over Electro-Mechanical Relays. Application Note: AN-145-R03, (USA).

Kumar, G., Jain, V., Gandhi, O.P. (2013) 'Availability Analysis of Repairable Mechanical Systems Using Analytical Semi-Markov Approach', *Quality Engineering,* 25(2), pp.97-107.

Kuo, W. and Zhu, X. (2012) 'Importance Measures in Reliability, Risk, and Optimization: Principles and Applications'. Chichester, UK: John Wiley & Sons.

Li, X. and Ding, W. (2010) Optimal Allocation Of Active Redundancies To k-out-of-n Systems With Heterogeneous Components. *J. Appl. Prob.* 47, pp. 254-263.

Meisel, W.S. and Schaeffer, P.C.H. (1969) 'Reliability in Digital Systems with Asymmetrical Failure Modes'. *IEEE Transactions on Reliability,* R-18(2), pp. 74-75.

Oliveira, L.F.S. (2008) 'PFD of higher-order configurations of SIS with partial stroke testing capability', in *Proc. European Safety and Reliability conference (ESREL)*, (Valencia, Spain), pp. 1919-1928.

Osewold, C., Büter, W., Garcia-Ortiz, A. (2014) 'A coding-based configurable and asymmetrical redundancy scheme for 3-D interconnects', in *Proc. 9th International Symposium Reconfigurable and Communication-Centric Systems-on-Chip (ReCoSoC)*, (Montpellier, France), pp. 1-8.

Pozsgai, P., Neher, W., Bertsche, B. (2002) 'Models to Consider Dependence in Reliability Calculation for Systems Consisting of Mechanical Components', in *Proc. 3rd International Conference on Mathematical Methods in Reliability (MMR)*, (Trondheim, Norway).

Rausand, M. (2014) Reliability of Safety-Critical Systems: Theory and Applications. Hoboken, NJ: John Wiley & Sons.

Rausand, M. and Høyland, A. (2004) *System Reliability Theory. Models, Statistical Methods, and Applications*. 2nd edn. Hoboken, NJ: John Wiley & Sons.

Roettjer, P. (2004) 'Life testing and reliability predictions for electromechanical relays, *Evaluation Engineering,* 43(6), pp. 58-61.

Rogova, E., Lodewijks, G., Lundteigen, M.A. (2015) Analytical formulas of PFD calculation for systems with non-constant failure rates, in *Proc. European Safety and Reliability conference (ESREL)*, (Zurich, Switzerland), pp. 1699-1707.

Rogova, E., Lodewijks, G., Calixto, E. (2017). Reliability Assessment of Safety Systems with Asymmetrical Redundancy Architecture. Submitted to the *International Journal of Reliability, Quality and Safety Engineering*.

Ross, S.M. (1996) *Stochastic Processes*. 2nd edn. New York: John Wiley & Sons.

Sharma, V.K., Agarwal, M., Sen, K. (2011) 'Reliability evaluation and optimal design in heterogeneous multi-state series-parallel systems'. *Information Sciences* 181, pp. 362–378.

Wang, Y. and Li, L. (2012) 'Heterogeneous Redundancy Allocation for Series-Parallel Multi-State Systems Using Hybrid Particle Swarm Optimization and Local Search'. *IEEE Transactions On Systems, Man, And Cybernetics—Part A: Systems And Humans,* 42(2), pp. 464-474.

"Without data you are just another
person with an opinion."
W. Edwards Deming (1900-1993)

Chapter 6

Practical estimation of failure rate function

As was mentioned in the Chapters 3-5, a Weibull distribution is used for the characteristics of degradation of mechanical components. Theoretically Weibull parameters can be taken from the Weibull databases and other reliability sources. However, the accuracy of calculations that use Weibull parameters from the databases is not high. They can be used for an approximate reliability estimation. Therefore if degradation data is available, it is desirable to obtain Weibull parameters.

The degradation can be related to: 1) physical parameters of the product (e.g., corrosion thickness on a metal plate) or 2) merely indicated through product performance (Bae & Kvam, 2008). The second type of degradation is considered in this Chapter. Degradation analysis is the statistical tool for making conclusion about the lifetime distribution on the basis of the available degradation data (Bae & Kvam, 2008).

Due to a lack of statistical data of degradation of mechanical components in escalators, elevators and moving walks, the failure rate functions of degrading components are obtained in this Chapter by using available data from cryogenic control valves of the CERN Large Hadron Collider. Although the practical estimation of failure rate function is performed in this thesis for cryogenic control valves, the same procedure can be used for estimation of failure rate function of hydraulic valves in hydraulic elevators for example.

Practical estimation of failure rate function has some issues. These issues are related to clarification of the failure mode, "cleaning" and filtering of raw degradation data, and development of an algorithm for diagnostics that will catch the degradation trend. The target of this Chapter is to answer to the fifth research question: how can the failure rate function be obtained practically?

Practical obtaining of the failure rate function is conducted in this Chapter by determination of Weibull parameters for degrading mechanical components in the wear out region of the bath tube curve. Obtained failure rate function is used for calculation of PFD_{avg}, PFH and R values on the basis of the developed window-based Markov method presented in Chapter 5.

Section 6.1 describes the experiment conditions: the task of the experiment, availability of data and description of failure modes. Types of valves used for the experiment are given in Section 6.2. Section 6.3 describes operating conditions of the equipment. Section 6.4 presents degradation and life data analysis of cryogenic valves and obtaining the Weibull failure rate functions. Usage of practically obtained failure rate functions for PFH calculation by using window-based Markov method is shown in Section 6.5.

6.1 Experiment conditions

The object of data monitoring is cryogenic valves. The final purpose of the experimental work is to obtain the failure rate functions for degradation process related to cryogenic valves. Subtasks of the experiment are listed below:

1) to study the records in the cryogenic logbook for 2015 and to select mechanical failures related to cryogenic valves;
2) to develop the diagnostic algorithms for identification of possible degradation;
3) to process the available signals by using the developed algorithms for the purpose to find a possible degradation;
4) to analyse correspondence between failures described in the cryogenic logbook, and obtained degradation results by using the developed algorithms;
5) to perform degradation analysis in accordance to the existing thresholds;
6) to perform life data analysis by using the results of degradation analysis;
7) to obtain the failure rate functions for different thresholds;
8) to apply the window-based Markov method by using obtained failure rate functions as input parameters.

Available data for the experiment is raw monitoring data obtained from position of cryogenic control valves. There are two types of signals that were available for the analysis. Signals are available in the database:

- xxxx.POSRST – request (or ‘0’). This signal means a request to change position. The value is analogue (in % of open/close valve)
- xxxx.POSST – feedback (or ‘1’). This signal means a feedback obtained from the position sensor informing about the current position of a valve. The value is analogue (in % of open/close valve)

The example of these signals is demonstrated in Table 6.1.

Table 6.1: Signals of feedback and request.

Date and time	**Position, %**	**Signal**
19-03-2015 13:49:56	100	0
19-03-2015 13:49:56	92,86	1
19-03-2015 13:49:57	92,89	1
19-03-2015 13:50:30	92,82999	1
19-03-2015 13:50:57	92,89	1
19-03-2015 13:51:03	92,95	1
19-03-2015 13:53:03	92,89	1
19-03-2015 13:53:12	92,82999	1
19-03-2015 13:53:13	92,77	1
19-03-2015 13:53:18	92,82999	1

The position (% of opening/closing) is measured by position sensor. The action of positioning is performed by the positioner of the valve. Therefore there are three possible classes of failures (when the feedback does not correspond to the requested value):

1) Failure (electronic or mechanical) of position sensor: wrong value of a valve position is related to the wrong data obtained from the position sensor;
2) Failure (electronic or mechanical) of positioner: valve is able to open and close but cannot do that because positioner does not work properly;
3) Failure of the mechanical part of the valve: unable to close/open. Example: malfunction of a slide in slide valves.

6.2 Types of valves

Two types of valves were analysed in this work: cryogenic control valves and slide compressor valves.

6.2.1 Cryogenic control valves (bellows)

The first group of valves that was analysed is cryogenic control valves. Cryogenic control valves are bellows valves. The positioner for this type of valves has a remote electronic part. The reason of this remote location is radiation in the tunnel that affects the electronic part. These cryogenic control valves control liquid helium (He) and are powered by compressed air. The line of compressed air supplies air to pneumatic positioners of many cryogenic control valves.

Signal of order (request) is sent by the positioner. The feedback obtained from a valve goes back to the positioner. Afterwards, feedback is processed in PLC that, as a result, produces a new request and sends it to the positioner.

Isermann gives a description of all possible failures of pneumatic and mechanical part of pneumatic valves. There are many possibilities to detect early faults. However not all of these signals are always available. 'The possibilities of early fault detection depend strongly on the available electrical signals' (Isermann, 2011). In this experimental work only two signals (order and feedback (%)) are available. The limited number of signals significantly reduces the possibility to catch early faults.

The positioner gives a possibility to have a request and a feedback in % of valve position. However not always the position (%) gives a possibility to detect early faults that can become a failure. In case of a lack of additional signals, many failures occur unexpectedly without any increase of difference between request and feedback. The lack of additional signals and information creates uncertainties in the analysis.

Degradation of cryogenic valves was analysed by using 3 methods: 1) analysis of speed of opening and closing of a valve; 2) 'luft' analysis (time between request and feedback when a valve changes direction); 3) analysis of % difference between request and feedback. 1) and 2) methods were applied to ~30 cryogenic control valves. The analysis showed only some deviations from normal behaviour and did not show a long term degradation. The third method

(3) was applied to the group of slide valves and showed good results with a long term degradation.

A few cryogenic control valves were analysed by using the third method. They showed a very stable behaviour in the analysis of % difference between request and feedback. For example, cryogenic control valve QRLAB_19L2_CV947 has a % difference between request and feedback less than 0.05%. Figure 6.1 shows that % difference is limited in the corridor [0.25%; 0.3%] almost for the whole 2015 year except the fault in March described in the cryogenic logbook as oscillations in the valve position. This graph shows a stable behaviour without observable degradation during the considered time period. However, it does not mean that there is no degradation. This can be clarified only by involving more sensors and also by consideration of a higher number of valves.

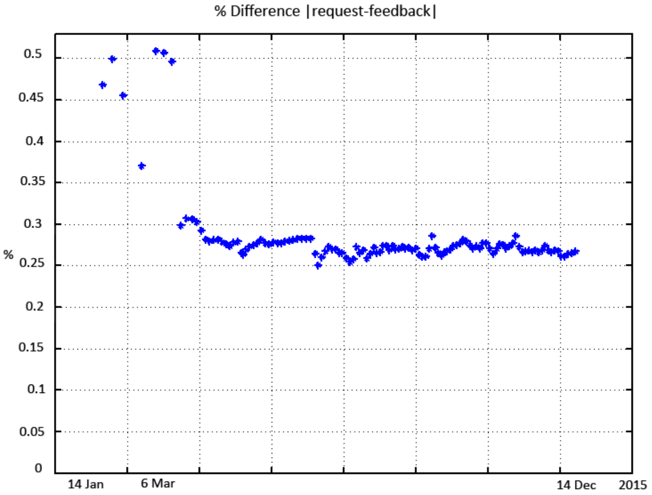


Figure 6.1: Difference between request and feedback for QRLAB_19L2_CV947.

6.2.2 *Slide valves (in compressor)*

Slide valves are the second group of valves considered in this study. ~25 valves of this type were analysed by using the third method (analysis of % difference between request and feedback). A slide valve is an oil-feed hydraulic valve. It is incorporated into the housing of a compressor station (see Figure 6.2). If the position of the control slide valve is changed, it leads to a corresponding orifice between the inlet – and the compression chamber. A proportionally larger or smaller volume of gas drawn into the machine flows back uncompressed to the inlet (Aerzen, 2012). The scheme of slide valve and screw compressor is shown in Figure 6.2.

In this study all degradations of slide valves CV120 are related to high vibrations of screw compressors because slide valves are incorporated into the compressors. The fasteners of position sensors of slide valves tend to gradually unscrew during the operation due to vibrations (based on the discussion with the expert of the cryogenic system). This requires frequent maintenance during the technical stops to avoid 'detaching' of position sensor and wrong values of position as a result.

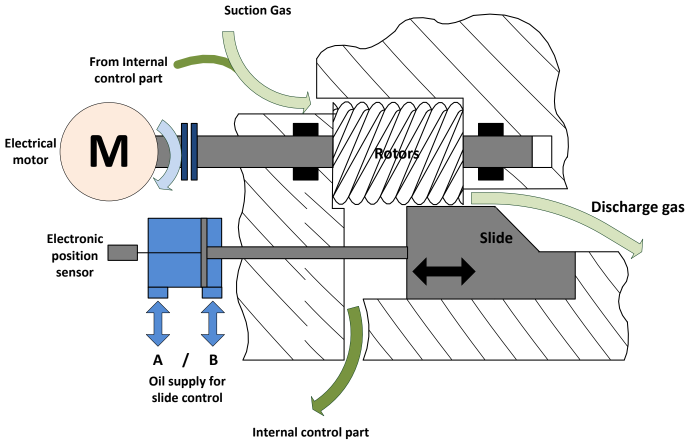
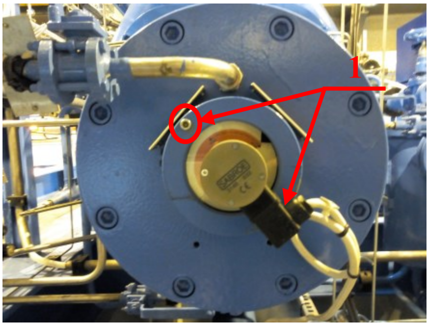

Suction Gas
From Internal control part
Electrical motor
M
Rotors
Discharge gas
Electronic position sensor
Slide
A / B
Oil supply for slide control
Internal control part

Figure 6.2: Slide valve in compressor housing.



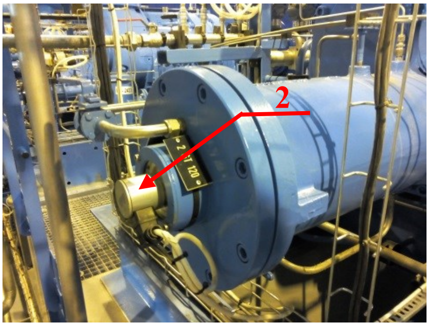


Figure 6.3: Slide valve inside of compressor housing; 1- fasteners of the position sensor; 2 – position sensor. Courtesy of CERN.

The photos of the valve, position sensor and compressor are presented in Figure 6.3. The position sensor is attached to the cylindrical body by two screws. These screws always need to be checked and tightened if vibrations unscrewed them. The slide valve is located inside the blue cylinder in Figure 6.3.

Degradation of equipment of systems of automation and control, especially in critical applications, cannot be considered separately only for mechanical part. The degradation analysis of a valve includes degradation of all related components (position sensors, positioner, connection line, regulators).

Analysis of available degradation data, the cryogenic logbook with description of failures, photos, schemes and manufacturer data, conducted in this study, revealed the component that makes the main contribution to decrease of reliability of a valve: the position sensor. If a position sensor does not give correct results, high reliability of a slide part of a valve is useless because functionality of a valve is governed by functionality of position sensor. The degradation analysis of a valve and a position sensor of a valve, cannot be considered separately.

6.3 Operating conditions

Operating conditions, technical stops and maintenance is very important for degradation analysis of cryogenic valves. This knowledge is required during the degradation analysis, for determination of the time slot, and for interpretation of obtained results after conducted analysis.

The raw monitoring data considered in this study are taken from the database of the year 2015. One year is sufficient for degradation analysis because degradation of valves between technical stops during this year is representative. That year had six technical stops (TS). Time intervals of these stops are listed in Table 6.2.

Table 6.2: Technical stops (TS) in 2015 (CERN LHC schedule 2015).

TS Before start	1 Jan- 30 Mar
TS check out	30 Mar-6 Apr
TS1	15 -19 Jun
TS2	31 Aug- 4 Sep
TS3	9-13 Nov
TS Xmas	14-18 Dec

During the TS the maintenance crew conducts repair, replacement and maintenance of the equipment if some malfunctions are found during the proof test of equipment. Often such predictive maintenance allows to avoid big failures on the stage of early faults. Predictive (condition-based) maintenance helps to reduce the amount of failures and corrective maintenance by early detection of failure symptoms. If the failure of a valve is critical and it leads to “loss of cryomaintain”, the machine will be stopped. If the failure is not critical, and there is no “loss of cryomaintain”, corrective maintenance cannot be conducted till the technical stop.

6.4 Degradation and life data analysis

11 slide valves are considered in this Chapter for degradation and life data analysis. These valves have different levels of degradation, but the same type of degradation described in Section 6.2.2.

6*.4.1 Degradation analysis*

The valve QSCB_6_2CV120 is the first valve considered in this group due to the failure described in the cryogenic logbook. Figure 6.4 (percentage difference between request and feedback) shows a failure that starts from small degradation and dramatically increases during several months.

The cryogenic logbook has a record related to this failure on 22 April 2015. The repair was conducted during the first technical stop TS1: position sensor was replaced. Due to vibrations of the compressors, the sensor was unscrewed, and it started oscillating. During TS1 the repair crew tightens fasteners and conducted visual inspection. As shown in Figure 6.4, vibration of compressor can significantly contribute to degradation of a valve.

The cryogenic logbook did not register any other failures related to this type of valves. However the 3rd type of analysis (difference between request and feedback) showed interesting results: degradation process (low or moderate) exists.

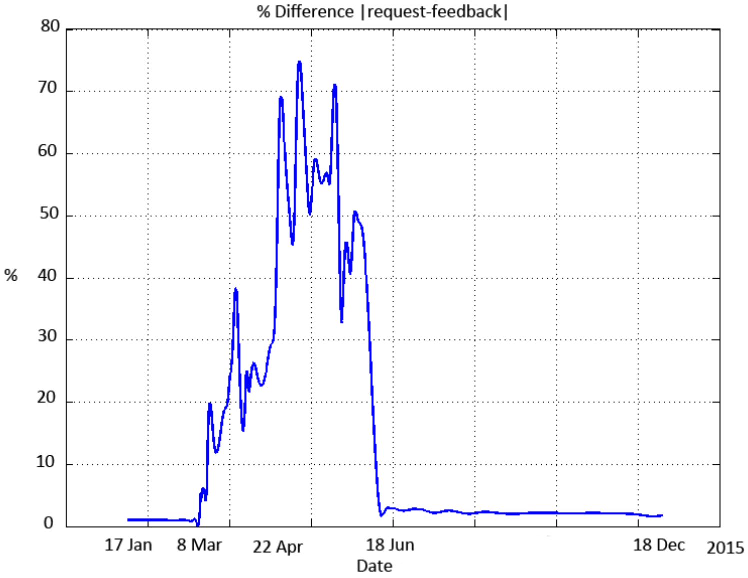


Figure 6.4: Absolute difference (%) between request and feedback for QSCB_6_2CV120.

The valves xCV120 are divided by two subgroups by location: valve from the cryoplant A (QSCA) and cryoplant B (QSCB). These valves are of the same type (slide valves), but they are produced by different manufacturers. Degradation and further Weibull analysis requires clear input parameters and identity of the investigating units. Therefore, due to different manufacturers for slide valves from the cryoplant A and cryoplant B, degradation analysis was conducted for these subgroups separately. The list of analyzed valves is available in Table 6.3.

Table 6.3: List of valves with degradation.

No	Valve name (Part A)	No	Valve name (Part B)
1	QSCA_2_7CV120	1	QSCB_18_3CV120
2	QSCA_2_8CV120	2	QSCB_4_2CV120
3	QSCA_4_1CV120	3	QSCB_6_1CV120
4	QSCA_4_2CV120	4	QSCB_6_2CV120
5	QSCA_4_3CV120	5	QSCB_8_6CV120
6	QSCA_4_8CV120		

The time period for the analyzed degradation is the same for all valves: 14.01.15-15.06.15. A bigger time interval is not considered here due to maintenance work during the technical stop TS1. Data available for the analysis, showed that some valves have degradation during the whole year 2015. Others – degrading till the technical stop, and after that start degradation again.

For processing the data from the database, program in Matlab was developed. The program is based on reading of raw data from Excel files, conversion to the required format, and calculation of difference between request (%) and feedback (%). In addition some "filtering" and "cleaning" of data was applied. Such filtering and cleaning of the raw monitoring data is considered in the example of the valve QSCA_4_1CV120. Figure 6.5 presents the result of calculation of difference between request and feedback for QSCA_4_1CV120 without any cleaning. Cleaning and filtering of the initial data are conducted here to remove the values of valve position "out of range": this is required to obtain the "clean" trend of degradation increasing without unexpected peaks. Further work with data is the averaging of "clean data". Figure 6.6 presents the result of filtering and cleaning the data with averaging: the interval 14.01-15.06.15 was divided into 40 small intervals, and average values were calculated for each small interval.

Figure 6.7 demonstrates averaged values of % difference between request and feedback for 6 valves in the cryoplant A, and 5 valves in the cryoplant B. Average values obtained by the first step of the analysis in Matlab were transferred to Weibull++ (Reliasoft software) for the second step: degradation analysis. Degradation plots for slide valves in cryoplant A and cryoplant B are presented in Figures 6.7-6.8.

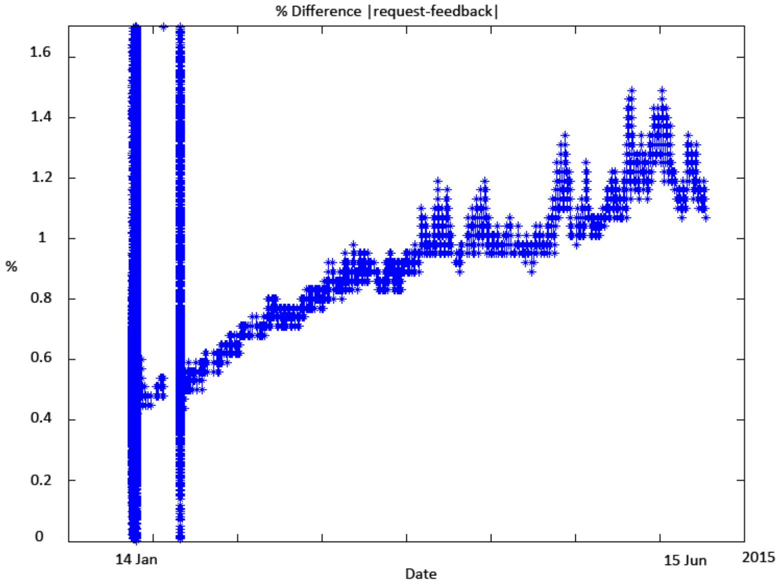


Figure 6.5: Difference (%) between request and feedback for QSCA_4_1CV120 without averaging and cleaning.

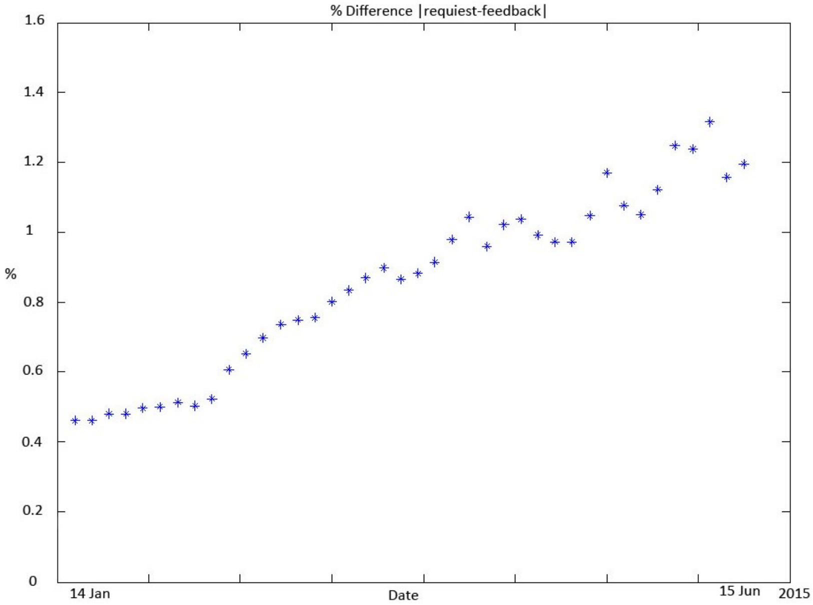


Figure 6.6: Average difference (%) between request and feedback for QSCA_4_1CV120 with applied cleaning of the data.

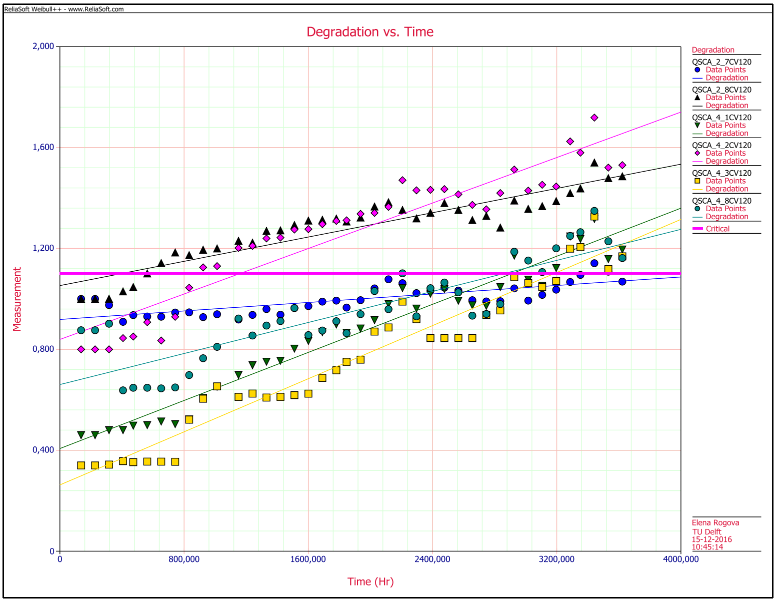


Figure 6.7: Degradation plot for 6 valves of CV120 type, cryoplant A: absolute difference (%) between request and feedback (critical value=1.1%).

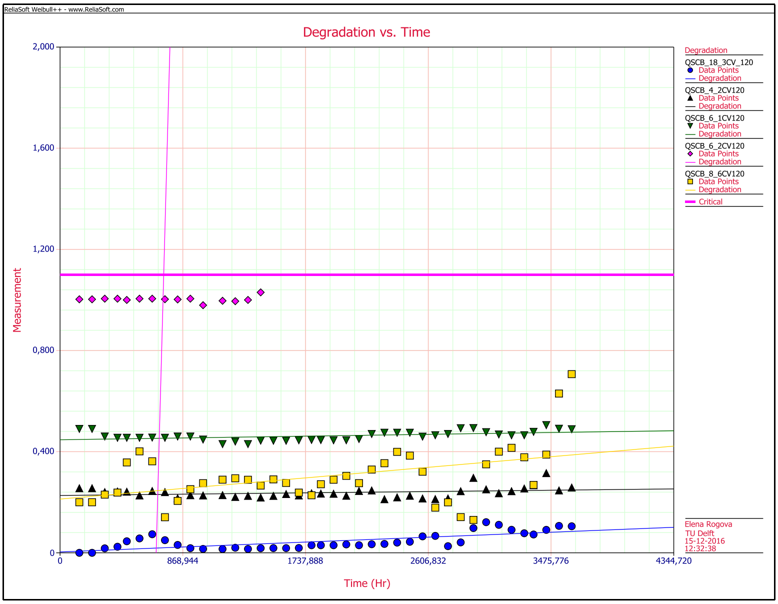


Figure 6.8: Degradation plot for 5 valves of CV120 type, cryoplant B: absolute difference (%) between request and feedback (critical value=1.1%).

The methodology to use degradation data as an input for life data analysis was investigated by Tobias and Trindade (1995), Nelson (1990), Bae & Kvam (2008) and others. The methodology of degradation analysis can be applied even if only a few failures exist. Test of degrading components do not need to be very long to obtain significant number of failures. Degradation for this analysis is defined "as a change of a specified magnitude in a parameter, regardless of its starting value" (Engineering Statistics Handbook).

Figures 6.7-6.8 present degradation curves and show also the line of critical degradation (threshold). Here it is equal to 1.1%. By comparison of several degradation models (linear, exponential and logarithmic) in Weibull++, linear degradation model showed the best fit to the data.

However, valves show degradation also in other time periods. Some of them recover due to the maintenance (by screwing fasteners of position sensor) during the technical stops. Others – continue degradation due to the lack of maintenance during the visual inspection. For example, QSCA_4_2CV120 has a trend of increasing of percentage difference between request and feedback for one year including technical stops.

Another example is QSCA_2_7CV120. It is interesting to analyze an additional graph of this valve without averaging for the period 14.09.15-17.12.15. The periodical increase of difference between request and feedback is demonstrated in Figure 6.9. This periodicity is clearly related to technical stops described in Section 6.3. After TS 3 difference between request and feedback reduces till 1%, and after that increases again.

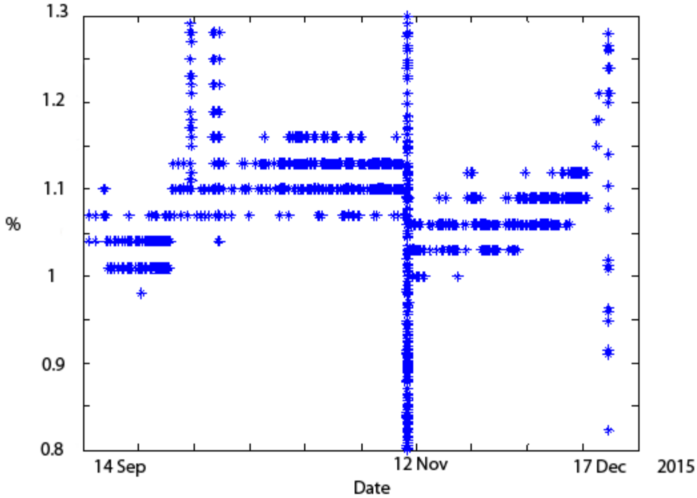


Figure 6.9: Absolute difference (%) request-feedback (QSCA_2_7CV120) for the period 14.09.15-17.12.15 without averaging.

6.4.2 Life data analysis

The next step after the degradation analysis is obtaining Weibull parameters by using the life data analysis. Values of Weibull parameters depend on the critical value. Several possible thresholds are considered here. These values are related to the maximally allowed difference between request and feedback: 1.1%, 1.2%, 1.5%. To see the difference between obtained Weibull parameters, the values of thresholds are taken slightly larger than 1% that was announced as a maximum allowed difference between request and feedback.

As a result of the degradation analysis the time to failure can be obtained. This time depends on the time when the degradation line crosses the critical value. If the line does not cross the critical degradation level during the specified test interval, the time of failure is obtained by extrapolation of a degradation data for each unit. Therefore for each group of valves (Part A and Part B) there are time values in hours that serve as input data for the life data analysis. The results of degradation and the life data analysis for the critical value=1.1% for QSCA valves are presented in Table 6.4.

Table 6.4: Results of Degradation and Life data analysis for QSCA valves (critical value =1.1%).

Distribution:	Weibull-2P		
Analysis:	MLE		
α	1,860714		
η (Hr)	2757,05865		
logLK Value	-51,647206		
Fail \ Susp	6 \ 0		
LOCAL VAR/COV MATRIX			
Var- α =0,439264	Var- η =397465,813784		
Raw Data			
Item Number	State F or S	Time to F or S (Hr)	Subset ID 1
1	F	392,1354794	QSCA_2_8CV120
2	F	1156,918971	QSCA_4_2CV120
3	F	2856,87939	QSCA_4_8CV120
4	F	2909,624947	QSCA_4_1CV120
5	F	3181,921604	QSCA_4_3CV120
6	F	4308,93412	QSCA_2_7CV120

The degradation analysis presented in the Figures 6.7-6.8 shows that data set contains units that did not cross the critical value during the observation time (3600 hours). Therefore, the initial data set can be considered as *right-censored* because “some units had a life exceeding the length of the test” (Wolstenholme, 1999). However, linear degradation model made by Weibull++ gave an approximate time of failure for all units that did not fail during 3600 hours. Therefore obtained times of failure for all units are considered as *complete data* with known parameters.

Obtained values of Weibull shape and scale parameters are obtained by using the software Weibull ++. The results of life data analysis are obtained by using MLE (Maximum Likelihood Estimation) method. For determination of confidence bounds, Fisher Matrix is used.

Table 6.5: Results of Degradation and Life data analysis for QSCB valves (critical value =1.1%).

Distribution:	Weibull-2P		
Analysis:	MLE		
α	0,808239		
η (Hr)	53737,25411		
logLK Value	-59,744348		
Fail \ Susp	5 \ 0		
LOCAL VAR/COV MATRIX			
Var- α = 0,097156		Var- η = 9,614486E+08	
Raw Data			
Item Number	State F or S	Time to F or S (Hr)	Subset ID 1
1	F	733,7557965	QSCB_6_2CV120
2	F	18416,54202	QSCB_8_6CV120
3	F	48924,17031	QSCB_18_3CV_120
4	F	79381,89411	QSCB_6_1CV120
5	F	146589,123	QSCB_4_2CV120

In case of complete data (as in current experimental study), the likelihood function is calculated using Equation 6.1 (Murthy et al., 2004). The values of *logLK* are shown in Table 6.4-6.7 by taking a logarithm of L(η,α).

$$L(\eta,\alpha) = \prod_{i=1}^{n}\left(\frac{\alpha t_i^{(\alpha-1)}}{\eta^{\alpha}}\right)\exp[-\left(\frac{t_i}{\eta}\right)^{\alpha}] \qquad (6.1)$$

The ML estimates should be obtained by solving the equations resulting from setting the two partial derivatives of $L(\eta,\alpha)$ to zero. As a result, estimate of shape parameter $\hat{\alpha}$ is obtained by solving the Equation (Murthy et al., 2004):

$$\frac{\sum_{i=1}^{n}\left(t_i^{\hat{\alpha}} ln\, t_i\right)}{\sum_{i=1}^{n} t_i^{\hat{\alpha}}} - \frac{1}{\hat{\alpha}} - \frac{1}{n}\sum_{i=1}^{n}\ln t_i = 0 \qquad (6.2)$$

The analytical solution for $\hat{\alpha}$ is unavailable. However it can be obtained by using computational methods. The scale parameter, therefore, can be estimated as (Murthy et al., 2004):

$$\hat{\eta} = \left(\frac{1}{n}\sum_{i=1}^{n} t_i^{\hat{\alpha}}\right)^{1/\hat{\alpha}} \tag{6.3}$$

The values of estimates of shape and scale parameters and logLK shown in Tables 6.4-6.7 have been checked by using the Equations 6.1-6.3.

The value of alfa α=1.78 presented in Table 6.4 clearly demonstrates the degradation for valves in Part A. However the value of alfa α =0.8 for valves in Part B shows approximately constant behavior because α ≈1 with account of standard deviation (Table 6.5). The prognostic time to failure is very large comparing to QSCA-valves (except a failure of QSCB_6_2CV120).

Valves of Part A are taken for further analysis due to their degradation with α>1. The life data analysis of the valves that do not show the degradation or show a very small degradation (QSCB valves), can be performed by other methods and using data provided by manufacturer. The results of degradation and life data analysis for slide valves in the cryoplant A for the critical values 1.2% and 1.5% are presented in Table 6.6 and Table 6.7 correspondingly.

Table 6.6: Results of Degradation and Life data analysis for QSCA valves (critical value =1,2%).

Distribution:	Weibull-2P		
Analysis:	MLE		
α	2,004910		
η (Hr)	3761,824219		
logLK Value	-52,880331		
Fail \ Susp	6 \ 0		
LOCAL VAR/COV MATRIX			
Var- α = 0,396553		Var- η = 656685,684751	
Raw Data			
Item Number	State F or S	Time to F or S (Hr)	Subset ID 1
1	F	1223,173257	QSCA_2_8CV120
2	F	1600,675601	QSCA_4_2CV120
3	F	3329,42024	QSCA_4_1CV120
4	F	3506,982272	QSCA_4_8CV120
5	F	3561,945329	QSCA_4_3CV120
6	F	6684,693169	QSCA_2_7CV120

By using Equation 2.1 (Chapter 2) the failure rate functions for different critical values can be obtained:

If the critical degradation $\Delta_{critical}$ = 1,5%, alfa=1.79, eta=6669 hours.

$$z(t) = 2.56 \cdot 10^{-7} \cdot t^{0.79}$$

If the critical degradation $\Delta_{critical}$ =1.2%, alfa=2, eta=3761.8 hours.

$$z(t) = 1.41 \cdot 10^{-7} \cdot t$$

If the critical degradation $\Delta_{critical}$ =1,1%, alfa=1.86, eta=2757 hours.

$$z(t) = 7.42 \cdot 10^{-7} \cdot t^{0.86}$$

For the test proof τ=3600 hours without repair (before TS1) the failure rate function is developing as shown in Figure 6.10.

Table 6.7: Results of Degradation and Life data analysis for QSCA valves (critical value=1,5%).

Distribution:	Weibull-2P		
Analysis:	MLE		
α	1,785755		
η (Hr)	6669,004065		
logLK Value	-56,611348		
Fail \ Susp	6 \ 0		
LOCAL VAR/COV MATRIX			
Var- α = 0,266435	Var- η = 2,643308E+06		
Raw Data			
Item Number	State F or S	Time to F or S (Hr)	Subset ID 1
1	F	2931,945492	QSCA_4_2CV120
2	F	3716,286591	QSCA_2_8CV120
3	F	4588,806121	QSCA_4_1CV120
4	F	4702,016504	QSCA_4_3CV120
5	F	5457,290918	QSCA_4_8CV120
6	F	13811,97032	QSCA_2_7CV120

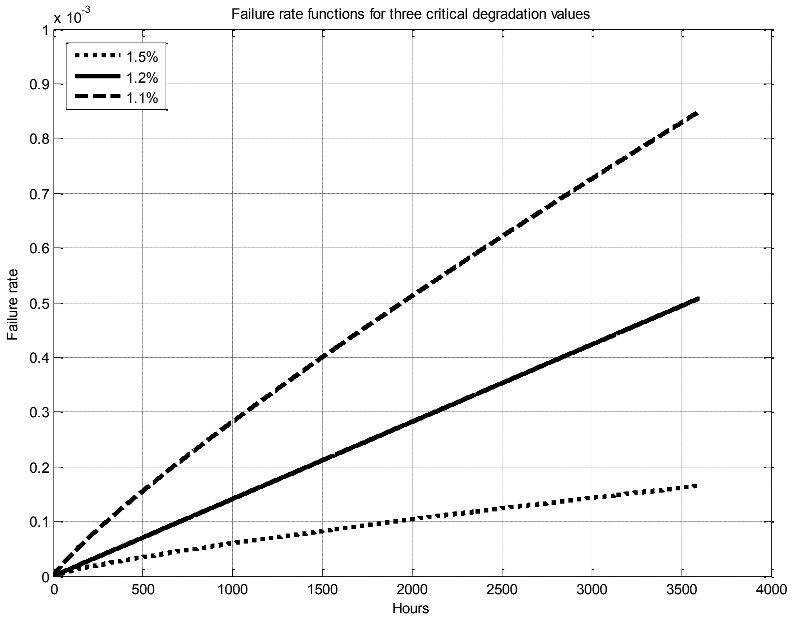


Figure 6.10: Failure rate function z(t) for 3 critical degradation thresholds.

Based on obtained data, the PFD_{avg} and PFH values can be estimated. For mechanical systems PFH value is calculated more often than PFD_{avg}. PFH value for the valves QSCA_x_xCV120 has to be calculated taking into account the obtained degradation without repair. In accordance to Section 4.4:

$$PFH_{1oo1}(\tau) = \frac{z(\tau)}{\alpha} \tag{6.4}$$

where 1oo1 represents the existence of only 1 channel without redundancy.

Therefore for τ=3600h without maintenance (see Chapter 4 for calculation of PFH):

For $\Delta_{critical}$ = 1.5%: PFH (τ=3600h)= $9.22\cdot10^{-5}$ h^{-1}
For $\Delta_{critical}$ = 1.2%: PFH (τ=3600h)= $2.54\cdot10^{-4}$ h^{-1}
For $\Delta_{critical}$ = 1.1 %: PFH (τ=3600h)= $4.56\cdot10^{-4}$ h^{-1}

Obtained PFH values do not have correspondence to SIL. If obtained results are not sufficient for the SIL requirements and not acceptable, there are several ways to enhance the reliability: to change the design (different fasteners), to change operating conditions (reduce vibrations) or to apply redundancy. In this study degradation is explained by operating conditions – vibrations of compressor. If fasteners of the position sensor have to be tightened during technical stops 3-4 times per year, it means that the fasteners or the whole body of a valve are not adapted for this level of vibrations. Probably, the solution of the problem is a different vibration-resistant fasteners of a position sensor. Change of operating conditions is impossible in this case due to the work of compressor (of course if the vibration level of compressor is in the allowed range). Application of redundancy can be considered as well. However this decision should be taken by account of cost and design constraints.

6.5 Application of window-based Markov method

PFH and PFD_{avg} values are normally calculated for safety-critical systems. Considered in this experimental study cryogenic valves are not a part of safety system because cryogenic system was not designed as a safety critical system. However, this Section shows calculation of PFH for the proposed redundancy architecture as one of possible ways to improve reliability. The goal of this calculation is demonstration of using the practically obtained failure rate function, and further calculations by using the window-based Markov method.

Reliability can be enhanced for example by inclusion another position sensor that have another type of fasteners and therefore will be resistant to the compressor vibrations. This can be done by using the 1oo2 redundancy architecture. In this architecture channel 1 is the old position sensor PS1 with fasteners that are affected by vibration: it has a non-constant failure rate z(t). Channel 2 is a new position sensor PS2 with new vibration-resistant fasteners. It can be a different manufacturer or different type of position sensor (inductive, magnetostrictive, linear displacement sensor etc.) with different type of fasteners to the body of a valve.

For the channel 2 inductive NAMUR sensor with a failure rate $\lambda_{PS2}=9.63\cdot10^{-9}$ (h^{-1}) was chosen (Aschenbrenner, 2004). For the channel 1 a failure rate function $z_{PS1}(t) = 1.41 \cdot 10^{-7} \cdot t$ is calculated for the critical threshold $\Delta_{critical}=1.2\%$. Calculation of such 1oo2 architecture is conducted in this Chapter by using the window-based Markov method presented in Chapter 5.

This system can have 4 states:

1) Channel 1 is OK, channel 2 is OK
2) Channel 1 is failed (F), channel 2 is OK
3) Channel 2 is failed (F), channel 1 is OK
4) Both channels are failed (F)

Therefore the simplified diagram of states (Figure 6.11) can be developed for the described 1oo2 redundancy architecture. Dangerous detected (DD) and dangerous undetected (DU) failures are not distinguished here. However if necessary, they can be simply included to the model by introducing the new states.

Therefore the system of Kolmogorov differential equations:

$$\begin{cases} \dot{P}_1(t) = \mu_{21}P_2 + \mu_{31}P_3 + \mu_{41}P_4 - P_1(\lambda_{12} + \lambda_{13} + \lambda_{14}) \\ \dot{P}_2(t) = \lambda_{12}P_1 - P_2(\mu_{21} + \lambda_{24}) \\ \dot{P}_3(t) = \lambda_{13}P_1 - P_3(\mu_{31} + \lambda_{34}) \\ \dot{P}_4(t) = \lambda_{14}P_1 + \lambda_{24}P_2 + \lambda_{34}P_3 - \mu_{41}P_4 \end{cases} \quad (6.5)$$

where P_i is a state probability.

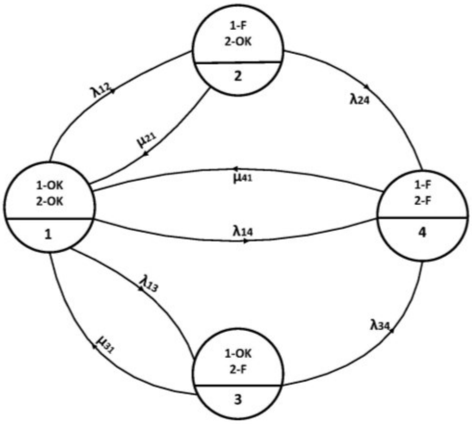


Figure 6.11: State diagram for the window-based Markov method.

Table 6.8: Failure and repair transition rates.

λ_{ij}	Expression	μ_{ij}	Expression
λ_{12}	$(1-\beta)z_{PS1}(t)$	μ_{21}	μ_{PS1}
λ_{13}	$(1-\beta)\lambda_{PS2}$	μ_{31}	μ_{PS2}
λ_{14}	$\beta \cdot \sqrt{z_{PS1}(t) \cdot \lambda_{PS2}}$	μ_{41}	$\mu_{PS1,PS2}$
λ_{24}	λ_{PS2}		
λ_{34}	$z_{PS1}(t)$		

where λ_{ij} is a failure rate corresponding to the transition i→j;
μ_{ij} is a repair rate corresponding to the transition i→j;
β is CCF factor that is equal to 0.05 due to possible influence of unscrewed fasteners of PS1 and vibrations to the reliability of position sensor PS2.

Taken into account that during the proof test interval repair cannot be conducted (only during the technical stop), all repair rates are equal to 0 here. For using the window-based Markov method the obtained failure rate function has to be discretized during the test interval. The test interval 3600 hours is divided into 6 equal discrete intervals by using the discretization model D2 (Chapter 5). Therefore the values of PFD, PFH and R (reliability) were obtained as follows:

$$PFH = 5.21 \cdot 10^{-8} \quad \text{(1/hour)}$$
$$PFD = 2.19 \cdot 10^{-4}$$
$$R = 0.99978.$$

6.6 Conclusions

This Chapter presented the degradation and life data analysis of valves in the cryogenic system at CERN. Conclusions obtained in this Chapter are listed as follows:

1. The analysis was conducted based on the study of available raw monitoring data, cryogenic logbook with description of failures, photos, schemes and manufacturer data for cryogenic control valves and slide valves. Cryogenic control valves did not show the observable degradation. Slide valves showed degradation.
2. The analysis of slide valves identified the component that made the main contribution to decrease of reliability of this type of valves: position sensor that was gradually detaching from the compressor housing due to vibrations. It was concluded that the position sensor had a crucial role in decrease of reliability of the slide valves.
3. Degradation and life data analysis of slide valves gave Weibull scale and shape parameters for three critical degradation thresholds: 1.1%, 1.2% and 1.5%. It was shown that values of Weibull parameters largely depend on the values of critical degradation thresholds.

4. Failure rate functions for all degradation thresholds showed high degradation that is reflected in obtained Weibull parameters: for instance for the threshold 1.2% α=2 and η=3762 h.
5. Practical obtaining of Weibull failure rate functions identified the issues related to determination of failure modes, cleaning and averaging of raw monitoring data, and knowledge about conducting maintenance. Therefore this Chapter gives an answer to the fifth research question: *How can the failure rate function be obtained practically?*

Failure rate functions obtained in this Chapter are used in the criterion of choosing the architecture that will be presented in Chapter 7. This choice of architecture takes into account reliability aspect, architectural constraints related to hardware fault tolerance and diagnostics, replacement costs, and system availability.

References

AERZEN screw compressors. (2012) *Aerzen Screw Compressors VMY with oil injection and integral capacity control for refrigeration series – 36*. AERZENER MASCHINENFABRIK GMBH. Available at: http://www.meacomp.com/pdf/aerzen2015/Oil-injected%20screw%20compressors%20VMY%20.36%20for%20process%20gas%20and%20refrigeration%20industry.pdf (Accessed 30 April 2016).

Aschenbrenner, S. (2004) *FMEDA and Proven-in-use assessment. Exida Project: Inductive NAMUR sensors.* Report No.: P+F 03/11-10 R015, Germany.

Bae, S.J., Kvam, P.H. (2008) *Degradation models.* In Encyclopedia of Statistics in Quality and Reliability. Wiley Online Library.

Bertsche, B. (2008) *Reliability in automotive and mechanical engineering*. Germany: Springer-Verlag Berlin Heidelberg.

CERN (2015). *CERN LHC schedule 2015.* Available at: https://espace.cern.ch/be-dep/BEDepartmentalDocuments/BE/LHC_Schedule_2015.pdf (Accessed 30 April 2016).

Engineering Statistics Handbook. *Fitting models using degradation data instead of failures.* Available at: http://www.itl.nist.gov/div898/handbook/apr/section4/apr423.htm (Accessed 8 December 2016).

International Electrotechnical Commission (IEC) (2011). *IEC 61810-2. Electromechanical elementary relays - Part 2: Reliability*.

International Organization for Standardization (ISO) (2008) *ISO 13849-1. Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design.*

Isermann, R. (2011) *Fault-Diagnosis Applications Model-Based Condition Monitoring: Actuators, Drives, Machinery, Plants, Sensors, and Fault-tolerant Systems*. Springer-Verlag Berlin Heidelberg.

Murthy, D.N.P., Xie M., Jiang R. (2004) *Weibull models*, Hoboken, New Jersey: John Wiley & Sons, Inc.

Nelson, W. (1990), Accelerated Testing, John Wiley & Sons, Inc., New York.

Rausand, M. (2014) *Reliability of Safety-Critical Systems: Theory and Applications*. John Wiley & Sons, Inc.: Hoboken, NJ.

Tobias, P. A., and Trindade, D. C. (1995), Applied Reliability, 2nd edition, Chapman and Hall, London, New York.

Wolstenholme, L.C. (1999). *Reliability modelling. A statistical approach*. Boca Raton, Florida: Chapman & Hall/CRC.

"Miser pays twice".
Russian folk wisdom

Chapter 7

Choice of architecture: reliability, availability, architectural constraints, and replacement costs

Based on the concept of functional safety presented in Chapter 3, by using the window-based Markov method developed in Chapter 5 and practically obtained failure rate functions, the decision scheme for the choice of architecture is presented in this Chapter. This decision scheme includes reliability assessment, architectural constraints, replacement costs, and availability calculation for the choice between a single component/subsystem and redundancy architecture.

Correspondence to SIL-requirements is the main issue at the design stage and during the operation of safety critical systems. If the component/subsystem does not meet the SIL requirements, the reliability has to be enhanced by increase of maintenance frequency, development of diagnostics or by applying redundancy. Sometimes the choice of architecture in not evident. For example the system after applying redundancy and a system without redundancy (but with a diagnostics), both can correspond to the required SIL during the test interval which is "the elapsed time between the initiation of identical tests on the same sensor, channel, etc." (Rausand & Hoyland, 2004). In this case further analysis should be conducted to make a final recommendation for the choice of architecture.

This Chapter is organized as follows. Section 7.1 proposes a decision scheme for the choice of architecture. The other Sections are parts of the proposed decision scheme. Section 7.2 contains architectural constraints on safety systems caused by hardware fault tolerance and safe failure fraction (SFF) – "fraction of the overall failure rate of a subsystem that does not result in a dangerous failure" (IEC 62061, 2005). Section 7.3 presents an availability calculation for a single component and an asymmetrical redundancy architecture. Section 7.4 discusses replacement costs. Section 7.5 concludes.

7.1 Decision scheme

The decision scheme (Figure 7.1) for the choice of architecture of a safety system is presented in this Section. The diagram starts from the existence of one single component/subsystem and goes through architectural constraints that include fault tolerance and SFF, sufficient values of PFD_{avg}/PFH and system availability, and takes into account replacement costs. The final goal of the decision scheme is to choose the appropriate architecture of a safety system.

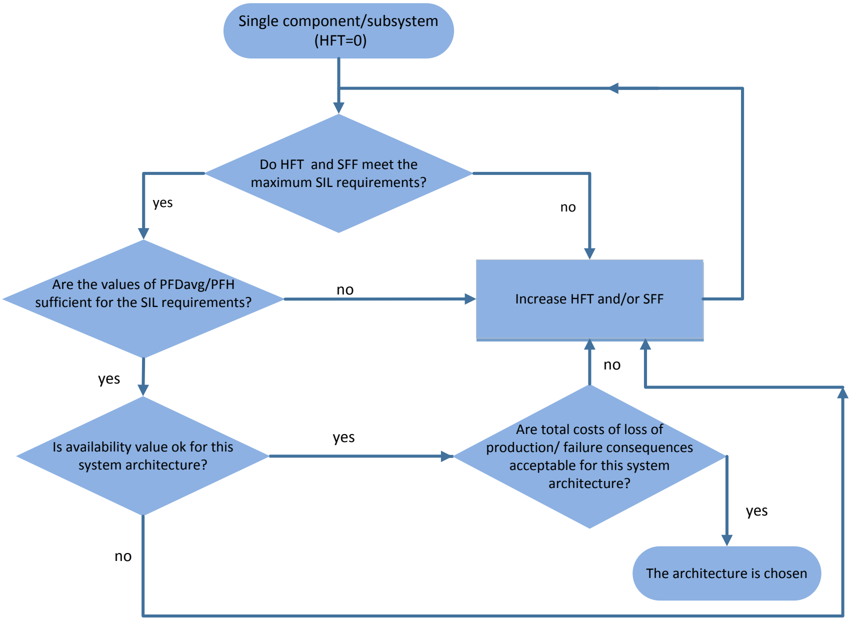

Single component/subsystem (HFT=0)
Do HFT and SFF meet the maximum SIL requirements?
yes
no
Are the values of PFDavg/PFH sufficient for the SIL requirements?
no
Increase HFT and/or SFF
yes
no
Is availability value ok for this system architecture?
yes
Are total costs of loss of production/ failure consequences acceptable for this system architecture?
yes
no
The architecture is chosen

Figure 7.1: Decision scheme for the choice between single component/subsystem and redundancy architecture.

The diagram shows the questions that have to be answered during the making a decision about the best architecture solution that meets the architectural constraints, SIL-requirements of IEC 61508 and related standards, system availability requirements and replacement costs (preventive replacement and failure costs) for the chosen architecture.

Next Sections consider all questions that have to be answered in the presented decision scheme starting from the architectural constraints and ending by replacement costs on the example of degrading slide valve with the failure rate function obtained in Chapter 6.

7.2 Architectural constraints

Architectural constraints of safety systems are considered by IEC 61508 in the framework of fault tolerance. Hardware fault tolerance (HFT) is defined as "ability of a functional unit to continue to perform a required function in the presence of faults or errors" (IEC 61508-4, 2010). There are different approaches to achieving fault tolerance. "Common to all these approaches is a certain amount of redundancy" (Dubrova, 2013).

HFT requirements have to be met at the system design stage. HFT together with Safe Failure Fraction define the maximum allowed SIL for the safety function performed by a safety-related component or subsystem. If the SIL assigned for the safety function is higher than allowed for this architecture, the architecture has to be changed by increasing HFT or/and SFF. The table of correspondence between SFF and HFT (Table 7.1) is presented by the IEC 61508 and adapted for the safety of machinery by IEC 62061 (IEC 62061, 2005).

HFT values are digit. For example, HFT=0 means that in case of fault, the safety function cannot be performed. HFT=1 means that in case of fault, one channel is unable to perform the function, but there is another one that can perform the function. Therefore the whole system is able to perform the safety function. For the redundancy architecture M-out-of-N, HFT=N-M that means that the safety system can tolerate (N-M) faults.

Table 7.1: Architectural constraints on subsystems: maximum SIL that can be claimed for a safety function carried out by a subsystem that comprises only a single subsystem element (IEC 62061, 2005).

SFF	**HFT**		
	0	**1**	**2**
< 60%	Not allowed	SIL1	SIL2
60% -<90%	SIL1	SIL2	SIL3
90% -<99%	SIL2	SIL3	SIL3
≥ 99%	SIL3	SIL3	SIL3

The formulas of SFF estimation for non-constant (a) and constant (b) failure rates are presented in Equation 7.1 (IEC 61508-4, 2010):

$$\text{(a)}\ \ SFF = \frac{\Sigma\lambda_{S\ avg}+\Sigma\lambda_{DD\ avg}}{\Sigma\lambda_{S\ avg}+\Sigma\lambda_{DD\ avg}+\Sigma\lambda_{DU\ avg}} \qquad \text{(b)}\ \ SFF = \frac{\Sigma\lambda_{S}+\Sigma\lambda_{DD}}{\Sigma\lambda_{S}+\Sigma\lambda_{DD}+\Sigma\lambda_{DU}} \qquad (7.1)$$

where λ_s is a failure rate of safe failure.

Although the right choice of HFT is necessary, it is not sufficient. Therefore a reliability calculation is required. If HFT=0 (lack of redundancy) has been preliminary chosen, and it has a high value of SFF that is ok for the required SIL, it does not mean that reliability calculations are not necessary. HFT defines only minimal architectural constraints: “It should also be noted that even if the hardware fault tolerance is achieved for all subsystems, a reliability calculation will still be necessary to demonstrate that the specified target failure measure has been achieved and this may require that the hardware fault tolerance be increased to meet design requirements” (IEC 61508-2, 2010).

The position sensor of the slide valve (Chapter 6), does not have diagnostics, and HFT=0 (no redundancy). On the basis of Table 7.1 the system cannot have SIL-requirements since it is not allowed. If the system has, for example, SIL1-requirements, it is allowed in case of applying redundancy even without existing a diagnostic system. Taking into account that diagnostics for the position sensor does not exist in the system, HFT=1 is minimal architectural requirements. Redundancy architecture 1oo2 suits these requirements.

It was shown in Chapter 6 that the slide valve with obtained Weibull parameters (α=2; η=3761.8h) does not correspond to SIL1. Therefore redundancy architecture has to be applied. Conducted calculations by using the window-based Markov method in Chapter 6 showed that the systems meets SIL1-requirements after applying redundancy. Therefore calculated reliability of a system meets SIL-requirements. The next step in the decision scheme is calculation of system availability.

7.3 Availability aspect

Most systems cannot operate continuously without stops caused by maintenance. In many cases, it is important to know not only the probability of failure, but particularly the time spent for repair/maintenance. (Dubrova, 2013). In application to equipment that transport people, it means that in case of a failure, the machine will be unavailable during the repair. In some cases it is unacceptable.

In public places with a big passenger flow, unavailability of the braking system of an escalator (and unavailability of the escalator consequently) can be critical. For example, if one of two escalators is unavailable during the peak hour, all passengers can use only one available escalator that can cause accidents. The similar example can be considered for elevators: in case of failure of car positioning for instance, the elevator is unavailable and people need to use another elevator if available that lead to increase of load of this elevator, or simply use stairs if another elevator does not exist. Therefore the question of availability of transport equipment is actual. However we distinguish here availability for passengers (that should include mean downtime to repair) and safety availability (or availability for safety). In this Chapter we consider safety availability.

“Availability is the ability of an item (under combined aspects of its reliability, maintainability and maintenance support) to perform its required function at a stated instant of time or over a stated period of time” (Rausand & Hoyland, 2004). The instantaneous availability at time t of a degrading component can be calculated as follows:

$$\mathrm{A(t)}= 1-\Pr(T\le t)=1-F(t) \tag{7.2}$$

The average safety availability of a component/subsystem can be of a larger interest than the instantaneous availability because it indicates safety availability of component/subsystem during a period of time (for example, test interval τ):

$$A = 1 - \frac{1}{\tau}\int_0^{\tau} F(t)dt = 1 - PFD_{avg} \quad (7.3)$$

For calculation availability of a redundant system with degradation the window-based Markov method proposed in Chapter 5, can be applied. In this case the average value of availability can be obtained by using the values of state probabilities of the last discrete interval *LDI*:

$$A^{LDI} = 1 - \sum_{i=1}^{q} P_i^{LDI} = 1 - PFD_{avg}^{LDI}, \quad (7.4)$$

where q is the number of states where the system is failed.

In the example with redundancy of the position sensor presented in Chapter 6, system unavailability is equal to the state probability P_4 at the sixth discrete interval in the state diagram (Figure 6.11). Calculated values of availability for systems with and without applying an asymmetrical 1oo2 redundancy are presented in Table 7.2.

Table 7.2: Availability values of the position sensor.

Availability	
without redundancy for a single degrading component	**with applying asymmetrical redundancy 1oo2**
0.6947	0.99978

Table 7.2 shows the big difference in values of average availability for the case with applying redundancy and for the case without applying redundancy. This example clearly proves the advantage of using redundancy in case of requirements on availability. If system availability is critical for a specific system, availability estimation can play a vital role in making a choice of architecture.

Availability of a system of redundant position sensors is high and supports the choice of redundancy architecture 1oo2. The next step in accordance to the decision scheme is calculation of replacement costs.

7.4 Replacement costs

In the problem related to the choice of architecture, replacement costs can be of interest for both cases: with and without applying redundancy. For instance, preventive replacement of a position sensor in a valve can help to save the valve itself. The cost of some valves can be very high especially in critical applications. Therefore preventive replacement of a position sensor can help to save money in case of a major failure of a valve itself and related costs of "loss of production".

Loss of production can be very critical in the process industry. If in case of a failure of a subsystem, the production process will be stopped, the loss can be very large. These losses are related to possible damage of other equipment and loss of money due to continuous production process which was stopped. Another type of losses should be considered in safety of machinery for machines that transport people. In this case major failures of safety systems can lead to the loss of people lives. The loss of money and loss of people lives are incomparable. That is why systems that do not have safety requirements can be considered in the scope of optimal replacement costs. However, the safety critical systems firstly have to be considered from the safety point, and secondly from the point of optimization of costs.

This Section presents the calculation of replacement costs for the age-based maintenance policy in the concept of optimal costs, and SIL-based maintenance policy for one component/subsystem with HFT=0 and for the redundant system with HFT=1. Age-based replacement costs were considered by many authors such as Rausand & Hoyland (2004), Blischke & Murthy (2003), Wolstenholme (1999). However usually replacement costs of one component/subsystem are in the scope. This Section compares replacement and failure costs of an individual degrading component and failure costs of a system after applying 1oo2 asymmetrical redundancy to the degrading components.

It is important to note that maintenance costs related to non-constant mean downtime are not considered here. However these costs can be obtained by applying the window-based Markov method with non-constant repair rates. In this case it is required to find a repair distribution (to model an increase of repair time depending on the age of the system). By discretization of failure and repair rates, the state probabilities can be obtained.

7.4.1 Failure costs for a single component/subsystem

An age replacement policy of a component/subsystem means its replacement upon a failure or at a specified operational age t_0. This policy normally takes place if the cost of a failure replacement is higher than the cost of preventive replacement, and the failure rate increases (Rausand & Hoyland, 2004).

The cost of preventive replacement of a component/subsystem before the failure has occurred is equal to c. The cost k is a failure cost: it is related to the loss of production in case of a failure of a component/subsystem, and $k>c$. It is important to note that failure costs have to be estimated and known before the failure has occurred. Therefore the total money expenditure for replacement of a failed component can be calculated as $c+k$. However the failure not necessarily has to occur in the selected replacement period, and the probability of this event (*Pr(failure)*) has to be estimated. Therefore the mean total cost C_{tot} for the selected replacement period can be calculated as follows (Rausand & Hoyland, 2004):

$$C_{tot} = c + C_f = c + k \cdot Pr(failure) = c + k \cdot \Pr(T < t_0) = c + k \cdot F(t_0) \quad (7.5)$$

where C_f – is failure costs

Therefore with account of frequency of replacements, the mean cost per time unit with replacement age t_0 (Rausand & Hoyland, 2004):

$$C_A(t_0) = \frac{c+k\cdot F(t_0)}{\int_0^{t_0}(1-F(t))dt} \quad (7.6)$$

If $t_0 \rightarrow \infty$, there is no age replacement, only corrective replacements take place with the cost of *(c+k)*. In this case $F(t_0) \rightarrow 1$, and $MTBR = \int_0^{\infty}(1-F(t))dt \approx MTTF$. Therefore:

$$C_A(\infty) = \lim_{t_0\rightarrow\infty} C_A(t_0) = \frac{c+k}{\int_0^{\infty}(1-F(t))dt} = \frac{c+k}{MTTF} \quad (7.7)$$

If the component has a Weibull distribution function of failure F(t) with Weibull shape (α) and scale (η) parameter, the cost ratio can be expressed as follows (Rausand & Hoyland, 2004):

$$\frac{C'_A(x_0)}{C_A(\infty)} = \frac{1+r\cdot(1-e^{-x_0{}^{\alpha}})}{\int_0^{x_0} e^{-x^{\alpha}}dx} \cdot \frac{\Gamma\left(\frac{1}{\alpha}+1\right)}{1+r} \tag{7.8}$$

where $x_0=t_0/\eta$ and r=k/c.

The task defined by the cost efficiency policy is to determine a replacement age t_0 that minimizes the ratio presented in Equation 7.8. The minimum value of this ratio $\left(\frac{C'_A(x_0)}{C_A(\infty)}\right)_{min}$ gives a value of x_0, and consequently, value of t_0 that gives a solution for a problem of finding an optimal cost-efficient time of replacement. The minimum of the ratio is difficult to get analytically. However it can be easily done by using a graphical approach.

Approximate preventive replacement/repair cost of the position sensor is estimated as *c*=€30. The failure of the slide valve does not lead to the loss of production. Therefore failure costs *(k)* are mainly related to the replacement of position sensor and maintenance work: these costs can increase till €90, €150, or €300 for example (different failure replacement costs are considered here). On the basis of Equation 7.8, the Figure 7.2 was built for three values of ratio between failure and preventive replacement costs: r=3, r=5, r=10.

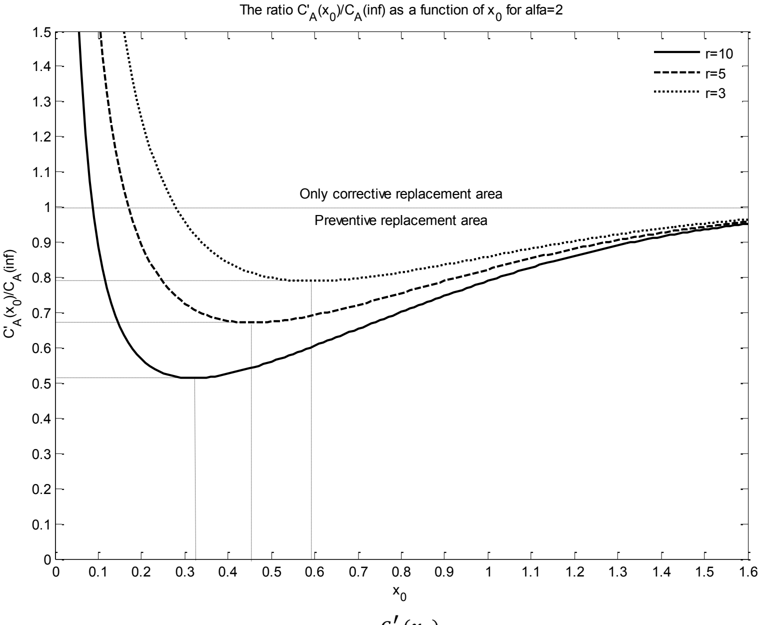


Figure 7.2: Cost function $\frac{C'_A(x_0)}{C_A(\infty)}$ for α=2, η=3761.8 h.

Figure 7.2 shows three cost functions for three different ratios between preventive and failure replacement costs *r*. By using this graphic, it is possible to obtain approximate values of the optimum cost measure. For example, for r=10, the minimum of the function is reached at x_0≈0.33 (see Table 7.4). The smaller the difference between *c* and *k*, the larger the value of x_0.

As was mentioned before, safety critical systems consider safety firstly, and cost efficiency secondly. Therefore it could be interesting to compare the time of age replacement t_0 and the maximum test interval τ_{SIL} before the SIL requirement is exceeded. Determination of τ_{SIL} is conducted here by calculation of PFH value for a single degrading component for different test intervals. By using Equations 4.29, the formula of PFH calculation for a single degrading component (architecture 1oo1) with Weibull parameters α and η can be obtained:

$$PFH^{1oo1} = \frac{\tau^{\alpha-1}}{\eta^{\alpha}} \tag{7.9}$$

On the basis of Equation 7.9 it can be calculated that the position sensor does not meet minimal SIL-requirements without applying redundancy (see Table 7.4). However for more reliable systems it is interesting to compare the time of age replacement and the maximum test interval τ_{SIL} before the SIL requirement is exceeded. Such comparison is presented here in Table 7.5 for a component with Weibull parameters α=1.5, η=6.67·10^5 h.

Table 7.4: Cost effective age- and SIL-based replacement for α=2, η=3761.8 h.

r	k,	c,	x_0^{min}	t_0, h	$\left(\frac{C'_A(x_0)}{C_A(\infty)}\right)_{min}$	τ_{SIL}, h			$\frac{C'_A(x_{SIL1})}{C_A(\infty)}$
	€	€				SIL3	SIL2	SIL1	
10	300	30	0.33	1283.2	0.51	--	--	--	--
5	150	30	0.45	1944.3	0.67				--
3	90	30	0.60	2644.2	0.79				--

Table 7.5: Cost effective age- and SIL-based replacement for α=1.5, η=6.67·10^5 h.

r	k,	c,	x_0^{min}	t_0, h	$\left(\frac{C'_A(x_0)}{C_A(\infty)}\right)_{min}$	τ_{SIL}, h			$\frac{C'_A(x_{SIL1})}{C_A(\infty)}$
	€	€				SIL3	SIL2	SIL1	
100	3000	30	0.07	46690	0.36	30	3000	297000	0.60
10	300	30	0.35	233450	0.72				0.73
3	90	30	0.84	560280	0.93				1.00

For the component presented in Table 7.5 comparison of τ_{SIL} and t_0 is interesting. If the required SIL is SIL3, the maximum test interval when PFH value exceeds 10^{-7} is τ_{SIL2}=3000 h. Therefore if system has SIL3 requirements, the maximum test interval ends much earlier in SIL-based policy (τ_{SIL2}=3000 h) than the time of age replacement t_0 ($t_0>\tau_{SIL}$).

The replacement/repair time is a minimum between test interval obtained by correspondence to the SIL value, and the time obtained by age-based replacement policy, if such replacement/repair is possible before the test interval ends:

$$t_{repl} = \min(t_0, \tau_{SIL}) \tag{7.10}$$

The total failure cost without account of frequency of replacement for the selected replacement period depends only on the probability of failure: the smaller the value of probability, the smaller replacement cost. For the position sensor considered in this Chapter and k=€300, the total failure costs are:

$$C_f(t_0 = 1283.2h) = k \cdot F(t_0) = €33 \tag{7.11}$$

7.4.2 Failure costs for a redundant system

The goal of this Section is to estimate the failure costs in case of applying redundancy architecture. If asymmetrical redundancy is applied, the channel with non-constant failure rate continue degradation as in the case with a single degrading component. However due to the redundancy by another channel with constant failure rate, the overall system reliability is significantly improved.

By using the discretization model D2, the test interval τ=3600 h was divided into 6 equal discrete intervals. Solving the system of differential equations gives 4 state probabilities for each discrete interval. t_0=1283.2 h in Table 7.4 corresponds to the discrete interval No3. t_0=1944.3 corresponds to the discrete interval No4. t_0=2644.2 corresponds to the discrete interval No5. For these discrete intervals the following state probabilities are obtained:

Table 7.6: State probabilities for the discrete intervals No3,4,5.

P_i	t_0=1283.2 h	t_0=1944.3h	t_0=2644.2
P_1	0.7271	0.6084	0.4936
P_2	0.2728	0.3914	0.5062
P_3	$1.19 \cdot 10^{-5}$	$1.31 \cdot 10^{-5}$	$1.32 \cdot 10^{-5}$
P_4	$1.08 \cdot 10^{-4}$	$1.47 \cdot 10^{-4}$	$1.83 \cdot 10^{-4}$

Since state probability P_2 is a failure of the 1st channel, P_3 – the failure of the 2nd channel, and P_4 – the failure of both channels (system failure), the failure replacement cost C_f can be obtained as follows:

$$C_f = k_1 \cdot P_2 + k_2 \cdot P_3 + k \cdot P_4 \qquad (7.12)$$

The following values are taken as failure costs for the redundant system: cost of failure replacement for the 1st channel (degrading) *k_1=€30*; cost of failure replacement for the 2nd channel *k_2=€30; k=€300* is the failure cost for the whole redundant system (will happen only when both channels fail).

Therefore the value of failure replacement costs at time t_0=1283.2h and *k=€300* is:

$$C_f(t_0 = 1283.2h) = €7.6 \qquad (7.13)$$

Comparison of the results presented by Equations 7.11 and 7.13 gives significant reduction of failure costs. If obtained failure cost for applied redundancy is acceptable, the redundancy architecture 1oo2 is approved. If the failure costs are not acceptable, hardware architecture can be reconsidered in accordance to the decision scheme.

Costs considered in Section 7.4 cover only preventive and failure replacement costs. However the costs of the initial design were not considered. For instance, one-off applying redundancy is more expensive than keeping operation of a single degrading component. At the same time the rejection of redundancy application in a favor of diagnostics can be even more expensive. The bottom line is that some diagnostics are much more expensive than applying redundancy. However, one-off money expenditure for the specific design (diagnostics and/or redundancy) will benefit in a long term of system operation at the expense of minimization of probability of dangerous failures and related failure costs.

7.5 Conclusions

This Chapter presented the decision scheme for the choice of architecture. Conclusions obtained in this Chapter are listed as follows:

1. The analysis performed in this Chapter showed four main contributors to the choice of architecture: 1) fault tolerance and safe failure fraction; 2) system reliability in accordance to SIL-requirements; 3) system availability; 4) costs of preventive and failure replacement.
2. HFT and SFF values with correspondence to the maximum allowed SIL assigned for the safety function define architectural constraints in accordance to IEC 61508. However further analysis of reliability, availability and replacement/repair costs can change this decision and lead to increase of HFT value.
3. If availability of a system with degrading component is critical, application of asymmetrical redundancy is recommended.
4. An asymmetrical redundancy architecture 1oo2 chosen to enhance reliability of position sensor of a slide valve showed higher reliability and availability values and smaller the values of replacement costs.
5. The replacement/repair time is a minimum between test interval obtained by correspondence to the SIL value, and the time obtained by age-based replacement policy, if such replacement/repair is possible before the test interval ends.
6. Total replacement (including preventive and failure replacement) costs were estimated for a single component and for an asymmetrical redundancy architecture by applying an age replacement, a SIL-based replacement policy and a window-based Markov method. It was concluded that in case of high cost of loss of production in process industry or possible injuries/deaths of passengers in case of failure in transport equipment, application of redundancy architecture is beneficial.

The decision scheme includes reliability calculation, availability aspects, architectural constraints and replacement costs in making a final decision for a choice between a single component/subsystem and redundancy. Therefore this Chapter answers to the sixth research question *"What is the criterion of choice of the architecture in systems with degradation?"*

References

Blischke, W.R. and Murthy, D.N.P. (2003) *Case studies in Reliability and Maintenance*. Hoboken, New Jersey: John Wiley & Sons, Inc.

Dubrova, E. (2013) *Fault-Tolerant Design*. New York: Springer Science+Business Media.

International Electrotechnical Commission (IEC) (2005) IEC 62061. Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems.

International Electrotechnical Commission (IEC) (2010) IEC 61508-2. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems.

International Electrotechnical Commission (IEC) (2010) IEC 61508-4. Functional safety of electrical/electronic/ programmable electronic safety-related systems. Part 4: Definitions and abbreviations.

Rausand, M. and Høyland, A. (2004) *System Reliability Theory. Models, Statistical Methods, and Applications*. 2nd edn. Hoboken, NJ: John Wiley & Sons.

Wolstenholme, L.C. (1999). *Reliability modelling. A statistical approach*. Boca Raton, Florida: Chapman & Hall/CRC.

Chapter 8

Conclusions and recommendations

On the basis of the research presented in the previous chapters, this Chapter sums up the main results achieved in this dissertation. Section 8.1 contains answers obtained for each research question described in Chapter 1. Recommendations for future research are presented in Section 8.2

8.1 Conclusions

This dissertation answers to the main research question introduced in Chapter1:
How to quantify the reliability of redundant safety systems with degradation?
To answer to this question two methods of reliability assessment were proposed in this dissertation: 1) analytical formulas of PFD_{avg} and PFH calculation were presented in Chapter 4 for solving the problem of PFD_{avg} and PFH calculation for redundant systems with degradation and identical channels; 2) the window-based Markov method was proposed in Chapter 5 to solve the problem of reliability assessment of heterogeneous redundant systems with non-identical channels and a combination of constant and non-constant failure rates.

To answer to the main research question it was necessary to consider 6 sub-research questions presented in Chapter1:

1) **Which methods and safety standards are available for reliability assessment of redundant safety systems?**

   In Chapter 2 it was shown that the methodology described in the safety standards gives only general guidelines from risk assessment and determination of the SIL requirements till reliability analysis and reliability enhancement. These safety standards do not have analytical formulas of reliability assessment that are applicable for safety systems with non-constant failure rates. Such analytical methods like RBD, Markov analysis, exact method, can be used for reliability assessment of redundancy architecture with identical channels and constant failure rates. A few analytical methods of reliability assessment are available for systems with identical channels and non-constant failure rates: the exact method and analytical formulas of the "ratio between CDFs". Heterogeneous redundancy architecture with different channels and a combination of constant and non-constant failure rates does not have analytical formulas of reliability assessment. Methods of reliability assessment that can be used for this type of architecture are mainly simulation. Petri Nets are applicable for this type of architecture. However it is a time-consuming complex method that is often used together with Monte Carlo simulation.

2) **How can the functional safety concept be used as a criterion for applying redundancy of a braking system of moving walks?**

Analytical formulas available in IEC 61508 are not applicable for PFD_{avg}/PFH calculation of systems with non-constant failure rates. Therefore only simplified approximate reliability assessment was conducted to obtain PFH values of a braking system for seven test intervals. Obtained in Chapter 3 PFH values of a braking system did not show the correspondence to SIL2. Proposed diagnostic system allowed to increase diagnostic coverage of a braking system and to achieve SIL-requirements. Calculation of PFH value after applying redundancy showed correspondence to SIL3 during 3 years and SIL 2 during 3-4 years of operation, which indicated significant reliability enhancement. Decision to apply redundancy was made in accordance to the functional safety concept on the basis of SIL-requirements as a criterion of not sufficient reliability of a braking system. In addition another field of application of functional safety concept was presented: it was concluded that design standards for bulk material belt conveyors should also address functional safety issues.

3) **Which analytical formulas can be developed for PFD_{avg}/PFH calculation of redundant safety systems with non-constant failure rates?**

Analytical formulas for PFD_{avg} calculation developed in Chapter 4 showed results that are very close to the results obtained by using the exact method

(Δ_{avg}=0.2%). Comparison of obtained simplified formulas of PFH calculation with full formulas also showed a very small difference (Δ_{avg}=0.4%) for all degradation effects in the considered case studies. Contribution from CCFs is significant for calculation of PFD_{avg} and PFH values especially in formulas of prognosis. Developed formulas of PFD_{CCF} and PFH_{CCF} showed increase each test interval. Obtained PFH formulas showed the same results for α=1 as formulas for the exponential case. Numerical results presented in Section 4.5 demonstrated the necessity of using a failure rate function for systems with strong degradation in the wear out region. Limitations of the proposed formulas, discussed in Section 4.6, require development of the new method that could cope with these limitations.

4) **How does the developed window-based Markov method overcome the limitations of the developed analytical formulas for reliability assessment?**

Comparison of the numerical results by the proposed method and by the steady-state semi-Markov method showed inapplicability of the steady-state semi-Markov method for the transient analysis. Comparison of the results obtained by window-based Markov method and results obtained by Monte Carlo simulation showed a very small difference for both non-repairable and repairable systems. The mean absolute error for non-repairable systems is 2% for discretization model D1 and 0.6% for discretization model D2. The mean absolute error for repairable systems is 2.2% for discretization model D1 and 1.1% for discretization model D2 for the considered case studies. Therefore in Chapter 5 it was concluded that discretization model D2 showed better results. Increase of number of discrete intervals makes closer the results of window-based Markov method and the results obtained by simulation. In the considered case studies the accuracy 99.4% (D2) for non-repairable and 98.9% (D2) for repairable systems is achieved by using 12 discrete intervals. The application of the proposed window-based Markov method can be limited only in case of large number of channels. In this case the number of system states in window-based Markov method can significantly increase that can create difficulties in calculation. Presented method overcame the limitations of analytical formulas presented in Chapter

4: window-based Markov method can be used if there is more than one component in a channel; it was shown that the method can be used for heterogeneous systems with non-identical channels and combination of constant and non-constant failure rates; the method is independent of the distribution chosen for the failure rate function.

5) **How can the failure rate function be obtained practically?**

The analysis was conducted in Chapter 6 based on the study of available raw monitoring data, cryogenic logbook with description of failures, photos, schemes and manufacturer data for cryogenic control valves and slide valves. Cryogenic control valves did not show the observable degradation. Slide valves showed degradation. The analysis of slide valves identified the component that made the main contribution to decrease of reliability of this type of valves: position sensor that was gradually detaching from the compressor housing due to vibrations. It was concluded that the position sensor had a crucial role in decrease of reliability of the slide valves. Degradation and life data analysis of slide valves gave Weibull scale and shape parameters for three critical degradation thresholds: 1.1%, 1.2% and 1.5%. It was shown that values of Weibull parameters largely depend on the values of critical degradation thresholds. Failure rate functions for all degradation thresholds showed high degradation that is reflected in obtained Weibull parameters: for instance for the threshold 1.2% $\alpha=2$ and $\eta=3762$ h. Practical obtaining of Weibull failure rate functions identified the issues related to determination of failure modes, cleaning and averaging of raw monitoring data, and knowledge about conducting maintenance.

6) **What is the criterion of choice of the architecture in safety systems with degradation?**

The analysis performed in Chapter 7 showed four main contributors to the choice of architecture: 1) fault tolerance and safe failure fraction; 2) system reliability in accordance to SIL-requirements; 3) system availability; 4) costs of preventive and failure replacement. HFT and SFF values with correspondence to the maximum allowed SIL assigned for the safety function define architectural constraints in accordance to IEC 61508.

However further analysis of reliability, availability and replacement/repair costs can change this decision and lead to increase of HFT value. If availability of a system with degrading component is critical, application of asymmetrical redundancy is recommended. An asymmetrical redundancy architecture 1oo2 chosen to enhance reliability of position sensor of a slide valve showed higher reliability and availability values and smaller the values of replacement costs. The replacement/repair time is a minimum between test interval obtained by correspondence to the SIL value, and the time obtained by age-based replacement policy, if such replacement/repair is possible before the test interval ends. Total replacement (including preventive and failure replacement) costs were estimated for a single component and for an asymmetrical redundancy architecture by applying an age replacement, a SIL-based policy and a window-based Markov method. It was concluded that in case of high cost of loss of production in process industry or possible injuries/deaths of passengers in case of failure in transport equipment, application of redundancy architecture is beneficial.

8.2 Recommendations

Results presented in this dissertation discover the recommendations for future research. These recommendations are presented as follows:

1) Development of the SIL assignment matrix specified for elevators, escalators/moving walks. This will require a detailed analysis of risks and accident consequences. Recommendations given in Chapter 3 and the template provided by IEC 62061 can be used as a basis.
2) Development of the updating procedure of Weibull failure rate function after repair of a degrading component. This research direction includes an update of Weibull parameters.
3) Comparison of PFH values obtained by using the Weibull failure rate function and the failure rate for cyclically operated components is of interest especially for those applications where determination of Weibull parameters is difficult.
4) Development of the CCF factor as a function of time: β(t). In this thesis β-factor is assumed to be a constant value for identical degrading channels. In the future research it is interesting to investigate possible increase of β-factor for different degrading channels.

5) Further development of analytical formulas of PFH calculation for systems with non-constant failure rates with account of dangerous detected (DD) failures.
6) Improvement of the developed window-based Markov method. The purpose is to reduce the large amount of system states in application to big safety systems with degrading components.
7) Application of the developed window-based Markov method in systems with non-constant repair rates. It is especially actual for those applications where the time spent for repair depends on some physical process. For example, in a cryogenic system when the time to recover the operability of a system (to cool down) depends on the initial temperature reached during the failure. This research is also interesting for estimation of maintenance costs when repair time is not constant and depends on the age of a system.
8) Investigation of other models of discretization for the window-based Markov method. In this dissertation the conservative (pessimistic) model was used. The future research can be conducted on study of discretization based on the average value.
9) The window-based Markov method was presented to practitioners, and they showed an interest in development of the software that employs this method for using in reliability assessment of systems with degradation. Therefore the development of such software can be considered as a potential research.

List of abbreviations

ALARP	As Low As Reasonably Practicable
BC	Brake Controller
BS	Braking System
CCF	Common Cause Failures
CDF	Cumulative Distribution Function
CEMA	Conveyor Equipment Manufacturers Association
DC	Diagnostic Coverage
DD	Dangerous Detected failures
DU	Dangerous Undetected failures
FMEA	Failure Modes and Effective Analysis
HAZOP	Hazard and Operability Study
HFT	Hardware Fault Tolerance
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LDI	Last Discrete Interval
LHC	Large Hadron Collider
LogLK	Log-Likelihood function
MC	Main Controller
MLE	Maximum Likelihood Estimator

MooN	M-out-of-N redundancy architecture
MP	Mechanical Part
MC	Main Controller
MRT	Mean Repair Time
MTTF	Mean Time To Failure
MTTR	Mean Time To Restoration
PFD_{avg}	Average Probability of Failure on Demand
PFH	Average Frequency of Dangerous failure per Hour
PL	Performance Level
PS	Position Sensor
RBD	Reliability Block Diagram
RBS	Braking System with Redundancy
ROCOF	Rate Of Occurrence of Failures
SCADA	Supervisory, Control and Data Acquisition
SCS	Safety Critical System
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SIS	Safety Instrumented System
TS	Technical Stop
1oo2D	1-out-of-2 architecture with additional diagnostic channels

Glossary

Symbol	Description
Latin lowercase	
a	Deceleration of moving walk
c	Preventive replacement costs
$f(t)$	Probability density function
k	Failure replacement costs
l	A value of allowable displacement of walking surface at rest condition
n_{op}	Number of operating cycles
r	Ratio between preventive and failure replacement costs
t	Time
t_0	Age-based replacement time in the concept of cost efficiency
t_1	The beginning of pulse from brake controller
t_2	The beginning of pulse from incremental sensor
t_3	The end of short pulse
t_4	The end of normal pulse
t_{per}	Time of periodic repairing
v	Current speed of moving walks
v_0	Final speed of moving walk
x_0	Ratio between age-based replacement time and Weibull scale parameter
$z(t)$	Failure (hazard) rate function

Latin uppercase	
A	Availability
A_k	Multiplier
B_{10}	Number of cycles until 10% of the components fail dangerously
$C_A(t_0)$	The mean cost per time unit with replacement age t_0
C_f	Total costs of replacement due to a system failure
C_{tot}	Total costs for preventive and failure replacement
D	Dangerous failure
$F(t)$	Cumulative distribution function
M	Minimum number of functioning channels in MooN redundancy architecture
N	Number of all channels in MooN redundancy architecture
N_{max}	Maximum number of pulses per revolution
N_θ	Minimum number of pulses per θ -rotation
P_i	State probabilities
R	Reliability
Greek lowercase	
α	Shape factor of Weibull distribution
β	Common cause factor
θ	Angular displacement
η	Characteristic life of Weibull distribution
λ	Failure rate

λ_0	Value of failure rate function for t_0=1 hour after the beginning of operation
λ_k	Value of failure rate function on kth discrete interval
λ_{ij}	Failure rate for transition between Markov states
λs	Failure rate of safe failures
μ	Repair rate
μ_{ij}	Repair rate for transition between Markov states
τ	Proof test interval
τ_{SIL}	Maximum test interval τ before the SIL requirement is exceeded

Greek uppercase

$\Delta_{critical}$	Critical degradation threshold

Samenvatting

Om passagiers veilig te kunnen vervoeren is het noodzakelijk dat transportequipment betrouwbaar is. Veiligheidssystemen in transportequipment vervullen veiligheidsfuncties binnen gespecificeerde grenzen ('safety integrity level', SIL). Als de betrouwbaarheid van een veiligheidssysteem te laag is, moet die worden verhoogd tot het gewenste niveau. Dit kan worden gedaan door beter onderhoud, door uitbreiding van de diagnostiek of door het aanbrengen van redundantie in het systeem.

Om te kunnen vaststellen dat de betrouwbaarheid wel of niet voldoende is, moet de waarde ervan worden berekend. Dat kan analytisch of met behulp van simulatie. Een te beperkt aantal simulaties leidt tot fouten in de resultaten. Daarom worden zowel door wetenschappers als door mensen uit de praktijk bij voorkeur analytische methoden gebruikt.

In dit proefschrift worden analytische methoden voor het berekenen van de betrouwbaarheid bestudeerd, in het bijzonder voor systemen die onderhevig zijn aan veroudering. Doordat bij systemen met veroudering de faalsnelheid niet constant is, zijn analytische methoden voor het berekenen van de betrouwbaarheid voor dergelijke systemen beperkt bruikbaar (in dit proefschrift zijn de faalkansen gemodelleerd met de Weibull-verdeling). De beperkingen van de analytische methoden worden in hoofdstuk 3 van dit proefschrift getoond in een voorbeeld van een remsysteem voor een rollend trottoir (loopband). Analytische methoden zijn in het algemeen alleen bruikbaar voor systemen met constante faalsnelheid; dit geldt in het bijzonder voor systemen met redundantie.

In dit proefschrift worden twee methoden gepresenteerd voor het berekenen van de betrouwbaarheid van redundante systemen met veroudering: 1) analytische formules en 2) een Markov-methode met tijdvensters ('window-based Markov method'). Analytische formules voor PFD_{avg} en PFH gaven goede, nauwkeurige resultaten. Deze vereenvoudigde formules kunnen erg makkelijk worden gebruikt, doordat er geen modelbouw voor nodig en en doordat het resultaat direkt beschikbaar is. Maar deze formules kunnen alleen worden gebruikt voor systemen met kanalen met gelijke verouderingskarakteristiek. De window-based Markov methode kan worden gebruikt voor redundante systemen met ongelijksoortige kanalen en een combinatie van constante en niet-constante faalsnelheden. Systemen met deze gemengde karakteristiek worden in dit proefschrift aangeduid als systemen met 'asymmetrische redundantie'.

Resultaten met de window-based Markov methode zijn gevalideerd door vergelijking met resultaten uit simulaties met Blocksim. Uit de vergelijking bleek een goede nauwkeurigheid (een fout kleiner dan 1%) zelfs bij een klein aantal intervallen. Deze methode kan met een goede nauwkeurigheid worden gebruikt voor zowel reparabele systemen als voor niet-reparabele systemen.

De beslissing over het verbeteren van de betrouwbaarheid van een systeem kan worden genomen in de ontwerpfase of bij het reviseren of moderniseren van het systeem. In dit geval kan redundantie van oude mechanische componenten worden aangebracht door gebruik van nieuwe electronische componenten met dezelfde veiligheidsfunctie. Met de window-based Markov methode wordt het mogelijk om analytische berekeningen uit te voeren aan de betrouwbaarheid van systemen met een dergelijke asymmetrische architectuur.

Het ontwikkelen van software voor gebruik van de window-based Markov methode kan onderwerp zijn van verder onderzoek. De belangrijkste voordelen van de methode zijn de mogelijkheid om verschillende toestanden van een systeem met veroudering te modelleren en de nauwkeurigheid van de resultaten te beïnvloeden door het aantal tijdvensters te wijzigen. De gegevens die nodig zijn om de window-based Markov methode te kunnen toepassen zijn de parameters van de verouderingsverdeling, zoals gedemonstreerd in hoofdstuk 6.

Bij het afleiden van faalfuncties uit beschikbare monitordata deden zich enkele problemen voor met betrekking tot de kwaliteit van de gegevens en een duidelijke definitie van de toestand 'fout'. Het bleek dat de belangrijkste oorzaak voor het afnemen van de betrouwbaarheid van de klep lag in het losraken van de positiesensor van de het huis van de compressor. Ook bleek dat de analyse van de levensduur erg afhankelijk is van de drempelwaarde die voor de kwaliteitsvermindering wordt gekozen. Voor het analyseren van monitordata op veroudering en levensduur van transportsystemen kunnen dezelfde procedures worden gebruikt, als dergelijke data beschikaar zijn.

Concluderend: in dit proefschrift wordt de betrouwbaarheid van verouderende veiligheid systemen bestudeerd, met de nadruk op het aanbrengen van redundantie. Er worden analytische methoden gepresenteerd voor het berekenen van de betrouwbaarheid, die in de praktijk kunnen worden gebruikt voor systemen met veroudering.

Summary

Reliability of transport equipment plays a crucial role in providing safety for passengers. Safety systems of transport equipment perform safety functions with assigned safety integrity levels (SIL). If the reliability of a safety system is not sufficient, it has to be improved till the required level. This can be done by improving maintenance, enhancement of diagnostics or by applying redundancy.

To conclude that reliability value is sufficient (or not), it is necessary to calculate its value before and after reliability improvement. Such calculations can be done analytically or by a simulation approach. Usually simulation approach is time consuming for a large number of simulations. Small number of simulations leads to an error in the results. Therefore analytical methods are often welcomed by both – scientists and practitioners.

This thesis investigates analytical methods of reliability calculation focusing on systems with degradation. Analytical formulas of reliability calculation have limitations for systems with degradation due to non-constant failure rates (in this thesis they are modelled by Weibull distribution). These limitations have been shown in the example of a braking system of moving walks in Chapter 3: analytical methods are mainly applicable only to systems with constant failure rates especially in the case of redundant systems.

This dissertation proposes two methods of reliability calculation of redundant systems with degradation: 1) analytical formulas and 2) window-based Markov method. Analytical formulas of PFD_{avg} and PFH showed good results with high accuracy. These simplified formulas are very easy to use because they do not require building a model, and allow to get the result immediately. However they work only for systems with identical degrading channels. Window-based Markov method can be applied to redundant voting systems with different channels and a combination of constant and non-constant failure rates that are introduced in this thesis as an asymmetrical redundancy.

Results obtained by applying the window-based Markov method have been validated by comparison of this method and results of simulation obtained in Blocksim. This comparison presented a very good accuracy (the error is

around 1%) even for a small number of discrete intervals. This method can be used for both non-repairable and repairable systems with a good accuracy.

The decision about reliability enhancement can be taken at the design stage or during the overhaul/upgrade of a system. In this case redundancy of the old mechanical components can be proposed by using the new electronic components which perform the same safety function. Reliability assessment of such asymmetrical architecture becomes possible analytically by applying the proposed window-based Markov method.

The window-based Markov method was presented to practitioners, and they showed an interest in development of the software that employs this method for using in reliability assessment of systems with degradation. Therefore software development for the window-based Markov method can be considered as a proposal for future research. The possibility to model different states of a system with degradation and to change accuracy by changing the number of discrete intervals are the main advantages of the method. The data required for the analysis by using the window-based Markov method is parameters of distribution that model the degradation as those ones that were practically obtained in Chapter 6.

Practical obtaining of failure rate functions by using available raw monitoring data identified some issues related to the data quality, and clear definition of the failure mode. It was investigated that the main contribution to the decrease of reliability of the slide valve was made by the position sensor gradually detaching from the housing of the compressor station. It was also shown that life data analysis highly depends on the established degradation threshold for the degradation analysis. The same procedure of degradation and life data analysis can be applied to the raw monitoring data of transport equipment if available.

In conclusion, this dissertation investigates the reliability assessment of degrading safety systems with the main focus on redundancy allocation. The thesis presents the analytical methods of reliability assessment that can be applied in practice to the systems with degradation.

Curriculum Vitae

Elena Sergeevna Rogova was born in Penza, Russia in 1988. She received the M.Sc. degree in Electronics and Automation of physical facilities at the National Research Nuclear University (MEPhI) in Moscow, Russia in 2012. Ms. Rogova was working in the area of Automation and Control (InSAT, Moscow), programming (MCST, Moscow and TREI GMBH, Penza) and interlock and reliability (ITER, Russian Domestic agency).

In 2013 Ms. Rogova was invited to take a Ph.D. position at the Department of Transport Engineering and Logistics at the Delft University of Technology, The Netherlands. Her main research interest is reliability assessment of heterogeneous redundant safety systems, stochastic modelling for reliability prognosis of degrading systems, and functional safety.

List of publications

1. Rogova, E., Lodewijks, G., Pang, Y. (2014) Application of standards in reliability prognosis of braking system of moving walks. Proc. *European Safety and Reliability conference (ESREL)*, Wroclaw, Poland, pp.1289–1297.
2. Lodewijks, G., Rogova, E. (2014) Safety integrity level requirements in the design of belt conveyors. Proc. *Conference on Belt Conveyor Safety (SafeCon)*. Boksburg, South Africa, 1-15.
3. Rogova E and Lodewijks G. (2015) Braking system redundancy requirements for moving walks. *Reliability Engineering and System Safety*, 133, pp.203–211.
4. Rogova, E., Lodewijks, G., Lundteigen, M.A. (2015) Analytical formulas of PFD calculation for systems with non-constant failure rates, in *Proc. European Safety and Reliability conference (ESREL)*, (Zurich, Switzerland), pp. 1699-1707.
5. Niemi A., Apollonio A., Begy V., Gutleber J., Sollander P., Penttinen J.-P., Rogova E. (2016) FCC availability studies. FCC week, Poster session, Rome, Italy. 11-15 April 2016.
6. Rogova, E. and Lodewijks, G. (2016) Methods of reliability assessment of heterogeneous redundant systems. Proc. *8th IFAC Conference on Manufacturing Modelling, Management and Control MIM 2016*, Troyes, France, IFAC-PapersOnLine, 49(12), pp.139–144.
7. Rogova E., Lodewijks G., Lundteigen M.A. (2017) Analytical formulas of PFD and PFH calculation for systems with non-constant failure rates. *Proc IMechE Part O: Journal of Risk and Reliabilit*y, special issue, pp.1–10.
8. Apollonio A., Begy V., Gutleber J., Martin Marquez M., Niemi A., Penttinen J.-P., Rogova E., Romero Marin A., Sollander P. (2016) Big Data Analytics for the Future Circular Collider Reliability and Availability Studies. The 22nd International Conference on Computing in High Energy and Nuclear Physics (CHEP), San Francisco, USA. 10-14 October 2016.
9. Rogova E., Lodewijks G., Calixto E. (2017) Reliability Assessment of Safety Systems with Asymmetrical Redundancy Architecture. Submitted to the *International Journal of Reliability, Quality and Safety Engineering*.