Braking system redundancy requirements for moving walks

Elena Rogova *, Gabriel Lodewijks

Department of Maritime and Transport Technology, Delft University of Technology, Mekelweg 2, 2628 CD Delft, The Netherlands

Abstract

The 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 new standard ISO 22201-2, the reliability of a braking system of a moving walk has to correspond to safety integrity levels SIL1 till SIL3. In order to determine the required safety integrity level, a reliability analysis of a braking system has been performed using a probabilistic method and the Weibull distribution model. This paper presents the results of this reliability analysis and shows 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 and less reliability degradation in time than compared to braking system designs without redundancy. Based on these results and using a probabilistic and diagnostics approach, a suggestion for an intelligent system for preventing failure in a braking system is presented in this paper. This system maintains a required safety level of the braking system of a moving walk and predicts possible failures of the braking system.

1. Introduction

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, there are still accidents in practice. Some of these have tragic consequences, including casualties. Many tragic accidents happen because 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 [1]. 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 [2].

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 were 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” [3]. This example demonstrates that it is not enough to just apply redundant brakes without a 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/repair 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 [2]. 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 [4]. 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 [2]. Hydraulic brakes allow proportional control easier than electromagnetic brakes. Their brake torque can be controlled proportionally by changing the oil pressure [2]. 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 [2]. 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 [5]. ThyssenKrupp suggested solutions of constant braking distance regardless of the load [6], 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 people 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” [7]. 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" [4]. "The load conditions and additional safety features should be agreed to between the manufacturer and the owner reflecting the traffic levels which exist..." [4]. 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 repair 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 h per day, 7 days per week like moving walks in Los Angeles World Airports [8]. 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 a moving walk in that case is possible only at a limited period of time. This is especially topical for airports and big malls. Therefore, the focus of this paper 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 the present work is to estimate safety integrity requirements for a braking system of moving walks, to develop a method of 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 work confirm the necessity of a redundant braking system for moving walks with described operating conditions. Introduced intelligent system will be able to maintain the necessary safety integrity level (SIL), not only for the braking system, but also for other technical systems with degradation of their reliability parameters over time. Two modes of maintenance will be discussed: economical and full. This approach can help project managers to choose the most appropriate mode of maintenance for their company.

The structure of the paper is organized as follows. Section 2 considers a method for determination of safety integrity requirements and a reliability analysis of a braking system of moving walks. This section also presents a redundancy architecture, diagnostic system and intermediate results. Section 3 gives general results, a comparison of obtained graphs of PFH increasing with/without redundancy and introduces an intelligent system for SIL maintaining. Section 4 presents conclusions, discussion and future work.

2. Theory and calculations

This section outlines the method of probabilistic (reliability analysis) and diagnostic approaches of failure prediction. Calculations presented in this section, illustrate a 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.

2.1. Method of SIL requirements determination

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 are 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 [9]. 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” [10]. For the first stage (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 in this paper. This method in a combination with risk graph method allows to qualify risk (intolerable, undesirable, tolerable, negligible) and to define the class of risk quantitatively to receive the value of SIL. An ALARP model is good for both a qualitative and a quantitative risk estimation [11]. To make a conclusion about the necessity of redundancy of a braking system, a quantitative risk estimation is implemented in this paper. It is important to mention that SIL should be defined for safety functions [10]. 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 will be conducted in this paper for this final safety function.

In accordance to the ALARP-model [12], four consequence levels of moving walks accidents are defined: catastrophic (Ca), major (Ma), severe (Se) and minor (Mi). Table 1 demonstrates correspondence between the duration of brakes unavailability and the consequences of an accident in relation to the amount of injuries/deaths. This table is an interpretation of Table 5 “Quantitative consequence categories” in the manual for APCS engineers “Risk analysis of technological system in Interlock system conception for ITER” [13]. The table is adapted for people transportation equipment and considers number of sacrifices instead of money cost like in the table developed for ITER.

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

Table 3 demonstrates how to define a risk class in accordance to ISO 22201-2. Obtained from Table 3 risk classes [14] can be transformed to safety integrity levels in accordance to IEC 61508-6. To demonstrate how to use the described method, specific values of brakes unavailability, accident consequences and occurrence probability in events were chosen. For estimation it was assumed that an average brakes unavailability is less than 1 day. The most frequent accident consequences are No significant injuries. Intersection of the column and the row of Table 1 gives consequence level Major. The number of accidents is about 1 per year, that allows to define the category of occurrence probability: Occasional (Table 2). Intersection of the column Severe and the row Occasional of Table 3 gives the risk class IIIC. Unfortunately, the standard ISO 22201-2 does not provide readers by table of correspondence between risk classes and SIL. Determination of a safety integrity level in this paper is conducted by means of a risk graph method, described in IEC 61508-5. Compared to a qualitative method, a risk graph method considers more possible situations, that allow to estimate SIL more accurately. The method determined that risk class IIIC corresponds to 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. It is important to mention that 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.

Described method of the determination of general integrity constraints for the braking system can be used for all subsystems of moving walks.

2.2. Reliability analysis method

The braking system of a moving walk consists of electromechanical, hydraulic and electronic devices. 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 because of 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 to simplified

<table>
<thead>
<tr>
<th>Category</th>
<th>Potential frequency for effect</th>
<th>Mean value per year per unit moving walk</th>
<th>Mean value for total (2000) population per year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>≥ 0.01</td>
<td>0.01</td>
<td>20</td>
</tr>
<tr>
<td>Probable</td>
<td>0.001–0.01</td>
<td>0.005</td>
<td>10</td>
</tr>
<tr>
<td>Occasional</td>
<td>0.0001–0.001</td>
<td>0.0005</td>
<td>1</td>
</tr>
<tr>
<td>Remote</td>
<td>0.00001–0.0001</td>
<td>0.00005</td>
<td>0.1</td>
</tr>
<tr>
<td>Negligible</td>
<td>&lt; 0.000001</td>
<td>4.1667×10⁻⁷</td>
<td>0.000833</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event probability</th>
<th>Accident consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Catastrophic</td>
</tr>
<tr>
<td>Frequent</td>
<td>IA</td>
</tr>
<tr>
<td>Probable</td>
<td>IB</td>
</tr>
<tr>
<td>Occasional</td>
<td>IC</td>
</tr>
<tr>
<td>Remote</td>
<td>ID</td>
</tr>
<tr>
<td>Negligible</td>
<td>IF</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Brakes unavailability</th>
<th>&lt; 1 h</th>
<th>&lt; 1 Day</th>
<th>&lt; 2 Days</th>
<th>&lt; 1 Week</th>
<th>&lt; 1 Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>No injuries</td>
<td>Mi</td>
<td>Se</td>
<td>Se</td>
<td>Se</td>
<td>Se</td>
</tr>
<tr>
<td>No significant injuries</td>
<td>Se</td>
<td>Se</td>
<td>Se</td>
<td>Ma</td>
<td>Ma</td>
</tr>
<tr>
<td>&lt; 5 Severe injuries</td>
<td>Ma</td>
<td>Ma</td>
<td>Ma</td>
<td>Ma</td>
<td>Ca</td>
</tr>
<tr>
<td>&lt; 10 and &gt; 5 Severe injuries</td>
<td>Ma</td>
<td>Ma</td>
<td>Ca</td>
<td>Ca</td>
<td></td>
</tr>
<tr>
<td>&gt; 1 Death and/or multiple severe injuries</td>
<td>Ca</td>
<td>Ca</td>
<td>Ca</td>
<td>Ca</td>
<td>Ca</td>
</tr>
</tbody>
</table>
blocks (components), is demonstrated on Fig. 1. Each block has its own data in terms of reliability [15]. 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.

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

The general equation for the calculation of the PFHs for a system consisting of serial blocks of RBD is [16]

\[
PFH_S = \sum_{i=1}^{N} PFH_i
\]  

Eq. (2) describes the reliability of the braking system being the sum of the reliability of the individual components:

\[
PFH_{BS} = PFH_{MC} + PFH_{BC} + PFH_{MP}
\]

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 requirements in terms of safety and fault-tolerance. The configuration of the brake and the main controller (BC and MC blocks) and the PFH of its modules are shown in Table 4.

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 of the braking system and to calculate the PFH function dependence on time. 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” [17]. Even so, although “there are many statistical distributions other than the Weibull, the log-normal distribution is the second choice for life data analysis” [18]. 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, it was concluded that a Weibull distribution is a good choice for this target. 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 [19]. Secondly, there are data bases with Weibull shape factors \( \beta \) and characteristic life \( \eta \) parameters for all main types of mechanical equipment that makes engineering calculations of reliability with Weibull very suitable. This distribution allows obtaining the cumulative distribution function as a function dependence on time \( t \), \( \beta \) and \( \eta \). By means of varying the values of \( \beta \) and \( \eta \) for different components the PFH function for the system can be obtained. Weibull distribution parameters can be obtained based on analysis of real statistical data. But because of current lack of such data, databases of Weibull distribution parameters (\( \beta \) and \( \eta \)) were used for approximate calculations of PFH function for mechanical part of braking system. Tables of Weibull parameters from the book “An Introduction To Machinery Reliability Assessment” and free database of Barringer & Associates, Inc. [20, 21] were used for this target. Nine main components of mechanical part of braking system were considered for Weibull analysis: cylinder, DC motor, solenoid valve, pump, check valve, relief valve, springs, braking disk and pads.

PFH functions for all components of the mechanical part PFH\(_{\text{MEC}}(t)\) were obtained from the equation of Weibull cumulative distribution function \( F_w(t)\) [18]:

\[
F_w(t) = 1 - e^{-\left(\frac{t}{\eta}\right)^\beta}
\]

where \( t \) is the time; \( \eta \) is the characteristic life or scale parameter, and \( \beta \) is the shape parameter. The parameters \( \eta \) and \( \beta \) are known characteristics for each mechanical component \( i \).

Because of non-constant failure rates of the mechanical part MP, Eq. (2) with constant PFH values has to be transformed to PFH function dependence on time:

\[
PFH_{BS}(t) = PFH_{MC}(t) + PFH_{BC}(t) + PFH_{MP}(t)
\]

This equation allows obtaining the PFH function for a braking system. To obtain PFH values, it is necessary to substitute values of parameter \( t \) in hours. For the calculation of the operational time \( t \) per day, where the brake is used for braking, it is necessary to know an average number of stops per day and the mean duration of braking process. For an estimation it was assumed that an average number of stops per day is 1.4. The mean duration of the deceleration process was defined taking into account requirements of standard EN 115–1. For a nominal speed 0.75 m/s [4] the deceleration of 1 m/s\(^2\) shall not be exceeded [4]. For an estimation of the stopping time it was taken that the deceleration \( a \) is constant.

\[
t = \frac{v - v_0}{a}
\]

where \( v \) is current speed; \( v_0 \) is final speed = 0; and \( a \) is deceleration.

This equation gives the operation time of the brake per day: \( t_{\text{day}} = \left(\frac{0.75 \text{ m/s}}{1 \text{ m/s}^2}\right) 1.4 \times 1 \text{ s} = 2.8 \times 10^{-4} \text{ h/day} \).

The PFH values of braking system (PFH\(_{BS}\)) were obtained in accordance to Eqs. (3) and (4) for seven periods of time: 1 month, 6 months, 1 year, 2 years, 3 years, 4 years and 5 years. These values are given in Table 5.

The obtained results demonstrate strong degradation in terms of reliability from SIL2 till no SIL. Table 6 shows correspondence between SIL and the PFH.

**Table 4**

<table>
<thead>
<tr>
<th>Module</th>
<th>PFH</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU 315-2 PN/DP</td>
<td>1.00E-08</td>
</tr>
<tr>
<td>IM Interface (CPU to 1/O) IM 151-8 PN/DP CPU</td>
<td>2.00E-08</td>
</tr>
<tr>
<td>Profinet</td>
<td>5.00E-09</td>
</tr>
<tr>
<td>SM-326 Digital Output Card</td>
<td>1.00E-08</td>
</tr>
<tr>
<td>SM-326 Digital Input Card</td>
<td>1.00E-08</td>
</tr>
<tr>
<td>SUM:</td>
<td>5.5E-08</td>
</tr>
</tbody>
</table>

**Table 5**

<table>
<thead>
<tr>
<th>PFH(_{BS}) (months)</th>
<th>PFH(_{BS}) (years)</th>
<th>PFH(_{BS}) (5 years)</th>
<th>PFH(_{BS}^2) (months)</th>
<th>PFH(_{BS}^2) (years)</th>
<th>PFH(_{BS}^2) (5 years)</th>
<th>PFH(_{BS}^3) (months)</th>
<th>PFH(_{BS}^3) (years)</th>
<th>PFH(_{BS}^3) (5 years)</th>
</tr>
</thead>
</table>
Table 6
Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation [9].

<table>
<thead>
<tr>
<th>Safety integrity level (SIL)</th>
<th>Average frequency of a dangerous failure of the safety function [h⁻¹] (PFH)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>( \geq 10^{-9} ) to (&lt; 10^{-8} )</td>
</tr>
<tr>
<td>3</td>
<td>( \geq 10^{-8} ) to (&lt; 10^{-7} )</td>
</tr>
<tr>
<td>2</td>
<td>( \geq 10^{-7} ) to (&lt; 10^{-6} )</td>
</tr>
<tr>
<td>1</td>
<td>( \geq 10^{-6} ) to (&lt; 10^{-5} )</td>
</tr>
</tbody>
</table>

The SIL estimated by a reliability analysis of the braking system has to correspond to SIL requirements (SIL2) as it was defined in Section 2.1 However, the Tables 5 and 6 show that after a few months of exploitation SIL2 reduces till SIL1, and even till no SIL that is not appropriate for SIL requirements. The system requires some arrangements to improve reliability and decrease degradation of parameters.

2.3. Reliability increasing method

Two ways of prediction of failure are considered in this paper: probability approach, described in Section 2.2 and “redundancy+diagnostics” approach, described in this section. The probability approach predicts economical costs for repair in the future (amount of equipment that should be replaced in future and approximately when). The “redundancy+diagnostics” approach gives exact time of repair of the braking system. Combination of these two approaches gives an increase of reliability and convenient maintenance, based on prediction.

The results of calculation of PFH function presented in Section 2.2 show the necessity of reliability enhancement that can be reached by means of applying redundancy. However, as it was described in the introduction, even three installed brakes can fail in case of a lack of appropriate diagnostics of the equipment. In this section 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 redundancy architecture for braking system voting logics KooN was chosen. “F system is an n-component system which fails when any k of its n components fail” [22]. The 1oo2D architecture was chosen for redundancy of braking system. This architecture is a partial case of k-out-of-n (KooN) 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 part of a diagnostic system (Section 2.4) 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 fault triggers, and detailed self-test and mutual channel diagnostics. In systems with 1oo2 architecture four channels work parallel: two main and two diagnostic. This can help to achieve the highest safety level and fail-safety [23]. A physical block diagram of the 1oo2D architecture is shown in Fig. 2.

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_{min} = 1.0 \times 10^{-10} \text{h}^{-1} [24] of the incremental sensor was added to all seven values of the PFH in Table 5 for a monosystem (single system without redundancy) for the calculation of the overall reliability of the system with redundancy.

The functional scheme of the diagnostics for a braking system with 1oo2D architecture is shown in Fig. 3. This scheme was developed based on the requirements of the standard IEC 61508-6 (Fig. 2) for 1oo2D architecture applied to a braking system of moving walks.

Fig. 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 logic 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 2.4 There are also input 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.

All the calculations of the redundant system were executed according to the standard IEC 61508-6. Formulas given by the standard are expressed via failure rates \( \lambda \). Reliability analysis of the monosystem however was conducted for the PFH. To obtain the PFH function for a system with redundancy it was necessary to transform the PFH values of the monosystem to failure rates: for a 1oo1 (monosystem is a 1oo1 architecture) \( \lambda_{ARS} = PFH \) [23]. General equation of PFH function dependence on time was obtained based on formulas given by the standard IEC 61508-6. Because of the current lack of real data, pessimistic values of parameters (diagnostic coverage, the fraction of undetected failures, proof test interval, etc.) were chosen for obtaining the PFH function for a braking system with an applied redundancy architecture. Values of the PFH_{max} for the system with redundancy for seven periods of time (from 1 month till 5 years) are demonstrated in Table 7.

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 “switching to redundant system”. Calculations, choice of sensors and principle of work of the diagnostic system are described in Section 2.4.

2.4. Diagnostics of braking system

As it 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 Eq. (6):

\[
a = \frac{360 \theta}{\pi d}
\]
where $l$ – a value of allowable displacement of walking surface at rest condition and $d$ – 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 [4]; 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 (Fig. 4). According to these data and Eq. (6), the angular displacement $\alpha$ is equal to $\approx 1^\circ$. Thus, the minimum number of pulses $N_\alpha$ corresponds to the amount of pulses per $\alpha$ and characterizes the rest condition. For an estimation of the $N_\alpha$, error of measurement of number of pulses was chosen as $\pm 1$ 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 Eq. (7) and is equal to 1440 pulses per revolution (Table 8):

$$N_{max} = 360 \times N_\alpha$$

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 [24]. The pulse shaper, installed before the main controller, transforms sine to rectangular pulses and gives the picture shown on Fig. 5.

The duration of the pulse is proportional to the rotational speed. In Fig. 5, $t_1$ is the beginning of the pulse from Brake

---

### Table 7

<table>
<thead>
<tr>
<th>PFH$_{\text{month}}$</th>
<th>PFH$_{\text{months}}$</th>
<th>PFH$_{\text{year}}$</th>
<th>PFH$_{\text{years}}$</th>
<th>PFH$_{\text{years}}$</th>
<th>PFH$_{\text{years}}$</th>
<th>PFH$_{\text{years}}$</th>
</tr>
</thead>
</table>

---

### Table 8

<table>
<thead>
<tr>
<th>Degree ((\alpha))</th>
<th>Pulses</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>360</td>
<td>1440</td>
</tr>
</tbody>
</table>

---

Fig. 3. Functional scheme of diagnostics for a braking system.

Fig. 4. Displacement of walking surface at rest condition.
controller when it issues the signal “STOP MACHINE”. The time \( t_2 \) is the beginning of the pulse from the Incremental sensor. The time difference \( (t_2 - t_1) \) is the period of time, in which it is necessary to control the efficiency of braking. Time \( t_2 \) 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 \( t_2 \) 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 \( t_2 \) for different loadings in real time. This function depends on the motor current. The more the current – the greater the loading. Thus, it is possible to derive a dependence between current and loading: the greater the loading – the later control pulse duration (starting from \( t_2 \)) will be started.

The time difference \( (t_3 - t_2) \) 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 \( (t_4 - t_2) \) is a duration of the 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. Results

Based on the obtained results for a monosystem (Table 5) and for a system with redundancy (Table 7) a graph of PFH dependence on time was built. The top part of Fig. 6 shows a trend for a monosystem, the bottom part of this figure shows a trend for a system with redundancy. Comparing the two trends, it can be concluded that redundancy improves the reliability of a braking system. It decreases the overall degradation of the parameters and meets the requirement of SIL2 for 1 year. Indeed, the “space” of SIL2 for a system with redundancy is much bigger than “space” of SIL2 for a monosystem. Fig. 6 also shows that the lines of the system with redundancy and a monosystem are starting not in the same point, which means that redundancy decreases PFH immediately in this case. The PFH of the system with redundancy is also increasing. Nevertheless the declination angle of the line for the system with redundancy is much less, and the rate of reliability decrease is smaller, than for a monosystem.

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. For example, Fig. 6 demonstrates that after 1 year of exploitation the braking system is not acceptable for SIL2 even in case of redundancy. Thus, \( t_{per} \) (time of periodic repair) is equal to 1 year in this case. It means that after 1 year system reliability level should be recovered to SIL2. The general idea of this intelligent system is to keep track of the safety level of 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 about the close “border” between SILs, a company should take action for improving the reliability parameters. In most cases after $t_{per}$ (Fig. 7) 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 repair. The “economical mode” of repair 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 (Fig. 8). The “full mode” (expensive) means repair of all the wear-out components with full system recovering till the previous level of reliability (Fig. 7). Fig. 8 demonstrates that the time between regular partial repairs of system components is reduced in “economic mode” of maintenance. The time $t_{per}$ is approximately constant in “full mode”.

4. Conclusions, discussion and future work

In this paper, based on a reliability analysis, the necessity of redundancy for a braking system of public service moving walks with described operating conditions was shown (see Fig. 6). Two approaches (reliability and diagnostics) of failure prediction and a special intelligent system for SIL maintaining of a braking system were suggested in this paper. Full and economical modes for maintenance of braking systems of moving walks were introduced. The described method (Section 2.1) of determination of the reliability requirements is not only developed for moving walks. It is also applicable for elevators and escalators. By means of variation of the consequences of an accident and brakes unavailability, tables of brakes unavailability and consequences of an accident can be obtained for other transportation equipment. This method of serial tables gives engineers, constructors and audit companies a suitable tool for determination of SIL requirements for safety functions 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 because of wrong data of accident consequences, duration of brakes unavailability and method of transforming of risk class to SIL. A reliability analysis (Section 2.2) showed the necessity of redundancy in braking systems. The described method of increasing the reliability (by using of 1oo2D architecture) showed good results demonstrated in Fig. 6. Moreover, this figure also shows the necessity of periodical maintenance every two months, while in case of a redundant and diagnostic system this time is 1 year.

As it was mentioned in the introduction, the problem of reliability of brakes of moving walks is topical. There are several engineering solutions regarding improvement of braking system [5,6]. And this is still developing. The authors consider intelligent braking systems and even claim that intelligent braking system should have redundancy within it [2]. However the justification of the necessity of a redundant braking system as a measure of reliability increasing was not considered in research until now.

Subsequent studies are being performed addressing the verification and the validation of the developed methods. In addition, this model will be spread to all safety systems of people transportation equipment (elevators, escalators, moving walks). The standard IEC 61508 gives only general requirements for SIL determination and recommendations for calculations. Exact correspondence between risk classes and SILs should be stated in safety standards for sector application. However, the standard ISO 22201-2 does not contain this correspondence. The development of correspondence between the occurrence probability of accidents, accident consequences and SIL for escalators, elevators and moving walks is a target of further research.

Acknowledgements

This research is financially supported by Lifinstutitut (P90863), Amsterdam.

References


