SAFETY INTEGRITY LEVEL REQUIREMENTS IN THE DESIGN OF BELT CONVEYORS

G. Lodewijks and E. Rogova

Delft University of Technology

ABSTRACT

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) is defined as a discrete number for specifying the safety integrity requirements of safety functions. This paper illustrates how the SIL of a belt conveyor can be used advantageously at the design stage. 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.

1. INTRODUCTION

Belt conveyors are commonly used for the transportation of bulk solid materials. When designing a belt conveyor, several design codes are taken into account, like the CEMA 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:

- 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.
- The high tension apparent in the belt is a source of elastic energy, also called potential energy. Although the belt is designed to withstand 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.
- 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.
- 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 safety issues. A safety integrity level (SIL) is defined as a discrete number for specifying the safety integrity requirements of safety functions. This paper illustrates how the SIL of a belt conveyor can be used in the design stage. The focus is on the stop safety function provided by the brake.

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 Youfu 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 Youfu 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).

The application of a functional safety model is important since it helps to determine the safety integrity level (SIL). SIL is a discrete level (one to four) for ’specifying the safety integrity requirements of the safety instrumental functions to be allocated to the safety instrumented systems’ (IEC 61511-1 2003). The highest and most reliable level is SIL4, the lowest level SIL1. 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. This model is well known in nuclear, chemical, civil and other branches of engineering. 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 16 600 US miners died during the five-year period from 1911 to 1915. This is 3 300 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+A1 (Continuous handling equipment and systems—Safety and EMC requirements for fixed belt conveyors for bulk materials), NEN-EN 12882 (Conveyor belts for 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’. 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. The technical committees responsible for the specific application sectors specify, where appropriate, the safety integrity levels in the application sector standards (IEC 61508-1, 2010). This means that it is necessary to develop such a 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.

3. SIL DETERMINATION

As mentioned in the previous paragraph, a SIL is defined for a safety function and not for a total system. Table 1 shows the range of Probability of a Dangerous Failure per Hour (PFH) per SIL level (IEC 61508-1, 2010). For example, the probability per hour that a safety function with safety integrity level 4 does not perform is less than 10^{-8}.

Safety integrity level (SIL)	**Probability of dangerous failure per hour (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 $<10^{-5}$

Table 1. Safety integrity levels – target failure measures for a safety function operating in high demand or continuous mode of operation

IEC 61508-1, 2010.

Since a SIL concerns a safety function, it is necessary to compose a list of safety functions and a list of safety related systems that perform the corresponding safety functions before determining the safety integrity levels. This begins by determining accident consequence categories. The related standards are IEC 61508-5 and ISO 14121-2 (Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods) that define four such categories: Minor (Mi), Severe (Se), Major (Ma) and Catastrophic (Ca) (IEC 61508-5 2010, ISO 14121-2 2012). Unfortunately, the standards do not explain how to delineate these categories. It is obvious that these definitions relate to possible damage or injuries/deaths of people as a consequence of an accident. Table 2 demonstrates an example of the correlation between the consequences of an accident (in injuries and deaths) and the unavailability of the brakes in a conveyor system (Rogova et al., 2014).

Consequences of an accident	Brakes Unavailability				
	<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
n_1 severe injuries	Ma	Ma	Ma	Ma	Ca
$>n_1$ and $< n_2$ severe injuries	Ma	Ma	Ma	Ca	Ca
$>=n_3$ death and/or multiple severe injuries	Ca	Ca	Ca	Ca	Ca

Table 2. Accident consequences

The parameters n_1, n_2, n_3 in Table 2 are values of possible injuries/deaths as a consequence of an accident with a belt conveyor owing to brake failure. For example, the consequence category of a brake being unavailable for more than one week without causing injuries is Severe (SE).

The next step after the determination of an accident consequences category is the determination of the occurrence probability in events per year (frequency of an accident). The standard IEC 61508-5 defines six frequency categories of risk classification of accidents: Frequent, Probable, Occasional, Remote, Improbable, Negligible. The values of the potential frequencies to these categories can be estimated based on statistical data of a company using belt conveyors or can, for example, be requested from related databases such as Mine Safety and Health Administration Accident, Illness and Injury Database (Mine Safety Database).

Category	Potential frequency for effect F	Mean value per year per unit belt conveyor	Mean value for total (N) population per year
Frequent	$F \geq F_1$	M_1	MT_1
Probable	$F_1 \leq F < F_2$	M_2	MT_2
Occasional	$F_2 \leq F < F_3$	M_3	MT_3
Remote	$F_3 \leq F < F_4$	M_4	MT_4
Improbable	$F_4 \leq F < F_5$	M_5	MT_5
Negligible	$F < F_6$	M_6	MT_6

Table 3. Occurrence probability in events per year

The parameters F1–F6 in Table 3 are values of potential frequency per year that should be defined by an engineer based on statistical data. The frequency category is required for the determination of a risk class. Different sector application standards suggest many variations of tables for risk class determination. Since belt conveyors don't have a sector application standard of functional safety or risk assessment, it is necessary to use the general recommendations of Standard IEC 61508. Table 4 presents an example of a risk classification, given by the Standard IEC 61508-5.

Frequency	Consequence category			
	Catastrophic	Major	Severe	Minor
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Negligible	IV	IV	IV	IV

Table 4. Example of risk classification of accidents

IEC 61508-5

The interpretation of risk classes helps to understand risk tolerability (Table C.2 in IEC 61508-5). Moreover, a risk class can be transformed into a SIL. Standard IEC 61508 suggests several options for SIL determination. A quantitative approach and a risk graph are but two methods. Standard IEC 61508, ISO 14121-2 and Annex A of Standard ISO 13849-1 recommend the risk graph method to determine SIL in the machinery sector. Input parameters for the risk graph method can be obtained from the Tables 2 – 4 of this paper.

As an example, assume that the brakes of a belt conveyor are unavailable for one day and that there are no significant injuries caused by the unavailability of the brake. From Table 2 it can be seen that the consequence category in this case is Severe (SE). If the frequency category is Occasional, (Table 3), then the risk class is III as shown in Table 4. This risk class is described by Standard IEC 61508-5 as a 'tolerable risk if the cost of risk reduction would exceed the improvement gained' (IEC 61508-5). If these input parameters are used for a risk graph method (Annex E of Standard IEC 61508-5) then the SIL level can be obtained. For example, assume that for a safety function the SIL was defined by the risk graph method as SIL2. This means that the reliability of a safety related system that performs this safety function also has to correspond to SIL2. This implies that the probability per hour that this safety function is not performed has to be less than 10^{-6} and more than 10^{-7}, (Table 1). It is important to note that the work of engineers determining SIL levels would be much reduced if a table of direct correlation between risk classes and SIL could be developed. This table however does yet not exist.

4. RELIABILITY ANALYSIS

A reliability analysis of a safety system can be conducted by using different methods. The choice of reliability analysis methods depends on many criteria: complexity of the system, whether the system is repairable or not, existence of dependent failure events etc. For more information see the Standards IEC 61508 and IEC 60300-3-1. A braking system of a belt conveyor is a repairable system. For the simplification of the calculations it is assumed that the time to repair a brake failure is quite small. It is therefore neglected. Note that in reality the time to repair a malfunctioning brake depends on the availability of a maintenance window, the availability of spares etc.

The principle of a reliability analysis can be demonstrated by a Reliability Block Diagram (RBD) method. A brake system (BS) of a belt conveyor can be presented as a set of blocks: a controller block (main and brake controller) and a mechanical part (hydraulic power unit, brake pads and brake Disc) (Rogova et al., 2014), see Fi

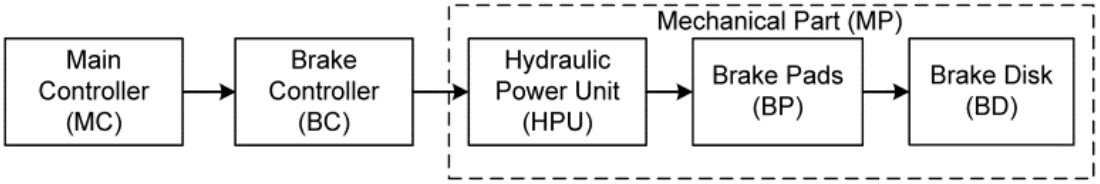

Figure 1. RBD of a belt conveyor brake system

The general equation for the calculation of the probability of a failure per hour (PFH) for the brake system consisting of the serial blocks of a RBD (N blocks) is IEC 61508-6 2010:

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

where *i* is the number of blocks. For a single component the PFH is equal to:

$$PFH_S = \lambda(1 - SFF) \qquad 2$$

where λ is the total failure rate of a component per hour and SFF the Safe Failure Fraction; the percentage of all failures that are not dangerous undetected. For the brake system at hand Equation 1 can be transformed to Equation 3:

$$PFH_S = PFH_{MC} + PFH_{BC} + PFH_{MP} \qquad 3$$

The chance PF_S that the brake fails within a certain period of time τ (hr) is:

$$PF_S = PFH_S\tau \qquad 4$$

For controllers, the PFH values can be calculated based on the specifications for these devices. The calculation of the PFH values of a mechanical part is much more difficult. The main difficulty is the non-constant failure rate. Because the strong degradation of the reliability parameters of a mechanical part, it is necessary to obtain a PFH(t) function instead of a constant PFH value (Rogova et al., 2014). As an example, the reliability of a brake pad of a caliper decreases in time during use. One of the methods that can be used to obtain a PFH(t) function is the probability distribution. In mechanical engineering the Weibull distribution is widely used as a suitable and practical tool. After obtaining the PFH(t) function of a mechanical part, it is necessary to calculate the PFH values for different periods of time and to display this in a figure. With the PFH(t) value at a certain point in time t and Table 1, the SIL of the safety function 'stop the belt conveyor' performed by the brake can be determined. This has to be compared with the required SIL determined in Section 3. If the calculated SIL is less than the required SIL then proper actions are required. Options are discussed later. It should be noted that with a decrease of PFH(t) in time, a brake that after installation has the right SIL may not have the required SIL as time passes. Certain actions in this case are also required.

5. THE RELIABILITY OF A BRAKE

Assume that a brake supplier quotes an operator of belt conveyors a mean time between failure (MTBF) of a (total) brake of 20 000 operations. Since the brake supplier is not able to give the PFH values for each brake component, Equation 1 cannot be used. However, Equation 2 can be used if the total failure rate per hour and the SFF are known for the brake as one system. From operational data of the operator's Enterprise Resource Planning (ERP) system, it is known that similar brakes are used 3 504 times per year. Therefore, the MTBF is equal to 20 000/3 504 = 5.71 years = 50 000 hours. The failure rate λ then is equal to 1/50 000 hours, which is 2.10^{-5} hr^{-1}. From the determination of the occurrence probability in events per year calculated by the brake supplier, see Section 3 for an example. The result was that the safe failure fraction of the brake is 83%. With Equation 2 it can be found that the PFH of the brake is $PFH=2.10^{-5}(1-0.83)=3.4.10^{-6}$ hr^{-1}. Table 1 shows the safety integrity level of the safety system (the brake in this case) corresponds to SIL1. In the previous paragraph it was assumed the SIL of the safety function performed by a brake should be SIL2. If that also holds for this brake then the SIL of the safety system of the brake offered by the brake supplier does not match the required SIL of the safety function. Therefore an alternative brake with a higher MTBF should be selected. To reach SIL2, the MTBF of the brake should be at least 68 000 hours. However, whether the required SIL of the safety function should be SIL1 or SIL2 depends on the risks involved with brake failure. If the belt conveyor is a regenerative downhill conveyor or a man-riding conveyor, then SIL2 may be required. If the belt conveyor is a yard conveyor on a dry bulk terminal then SIL1 may be sufficient.

Normally the operator services the brakes on his belt conveyors once a year. The probability of failure of the brake PF_S can be calculated using Equation 4. The result is shown in Table 5. Annual maintenance results in a probability failure of 2.93%. The impact of decreasing the maintenance interval can be seen in Table 5.

Inspection interval (hr)	**Probability of failure PF_S([-)**
Never (∞ hr)	100 %
Annual (8 760 hr)	2.93 %
Quarterly (2 190 hr)	0.74 %
Monthly (730 hr)	0.25 %
Weekly (168 hr)	0.06 %
Daily (24 hr)	0.01 %

Table 5. Probability of failure versus inspection interval

In the example given above it was assumed that the PFH is a constant value, not a function dependent on time. In practice however, the PFH will not be constant as there is degradation of mechanical components in the brake, like the brake discs.

To deal with a an irregular PFH, a SIL-based method can be used in determining the appropriate maintenance procedure for a belt conveyor braking system. Two maintenance modes are suggested here: full maintenance and economical

maintenance. Figure 2 demonstrates a simplified graph of the safety integrity level of the safety function performed by a brake system in a full mode. It is assumed that the brake is equipped with sensors that can track the degradation of the brake components. If, because of degradation of a specific component, the safety integrity level of the safety function performed by the brake is about to fall below the minimum required level, then the operator receives a signal that maintenance is required. The time of periodical maintenance (repair, replacement) is t_{per}. Note that t_{per} is an approximately constant period for a full mode. It depends on the degradation processes of a brake. In full maintenance mode, the recovery of a brake system is conducted until the initial value of reliability, or better still, the original safety integrity level of the safety function. In an economical maintenance mode (Figure 3) the recovery of a system is not full. This means that the brake is partly repaired or that the most critical and unreliable components are replaced. In every cycle t_{per} is reduced in an economical maintenance mode. However, this mode can be more cost effective and more appropriate for some operators.

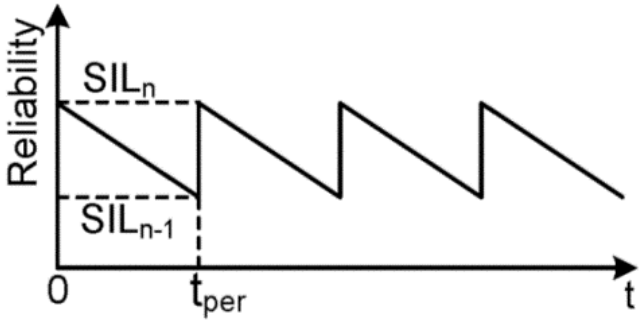

Figure 2. Simplified graph of work of an intelligent system in a full mode

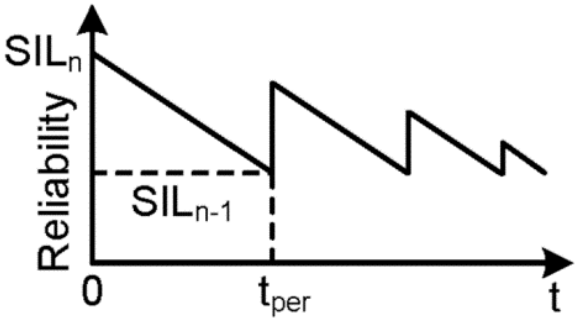

Figure 3. Simplified graph of work of an intelligent system in an economical mode

6. SAFETY IMPROVEMENT MEASURES

Three measures can be explored in order to improve the reliability of belt conveyor systems; adding redundant components, changing the architecture of safety systems, and adapting the maintenance strategies. An example of the latter has already been given in the previous section.

6.1 Redundancy of components

In the conventional engineering approach, safety related design issues are addressed by using redundancy of components or subsystems to achieve higher safety and reliability. Normally, redundancy can be dual, triple or quadruple. However, even though redundant systems may seem to lead to a serious increase in safety and reliability, in practice their impact may be limited. This is due to the fact that, with the installation of redundant systems, implicit assumptions are made:

1. There are no common parts shared between the redundant components or systems.
2. Only one system will fail at a time.
3. When one system fails it will be repaired immediately.

Assumption 1 in many cases is not valid because, for example, brake systems can share components like hydraulic lines. If such a line fails, the whole system fails. Assumption 2 may also not be valid in practice depending on the location of the redundant systems. If, for example, a dump truck drives into a belt conveyor it may destroy the original brake and the redundant brake at the same time. It also depends on the question of whether the redundant brake is on standby mode or also in operation. Finally, the validity of Assumption 3 depends on the maintenance strategy of the company using the system, the available maintenance window, and the availability of spares.

6.2 Architecture of safety systems

It is important to realize that the architecture of safety systems has a significant impact on the safety integrity level that a safety function can achieve. Table 6 lists the characteristics of the different architectures. A typical one channel one out of one architecture (1oo1) is shown in Figure 1. One out of one architecture means that the system at hand has one safety system. The system can fulfill the safety function only if this one safety system is in operation. If it is not in operation then the safety function cannot be fulfilled. Therefore the one out of one safety system has to work. A typical 1oo2 architecture is shown in Figure 4. In this case there are two separate brakes, two separate brake controllers (for example SOBO controllers) and one main controller. A one out of two architecture means that there are now two safety systems that can both fulfill the one safety function. Therefore, if one out of the two safety systems is operating correctly, then the safety function can be fulfilled. Adding a monitoring or diagnostic system to the safety system can further increase the reliability of the system. The diagnostic system detects the functional reliability of a safety system and initiates a switch from using the one safety system to the other if required. Figure 5 shows an example of a 1oo2 architecture with diagnostics, in this case denoted as 1oo2D.

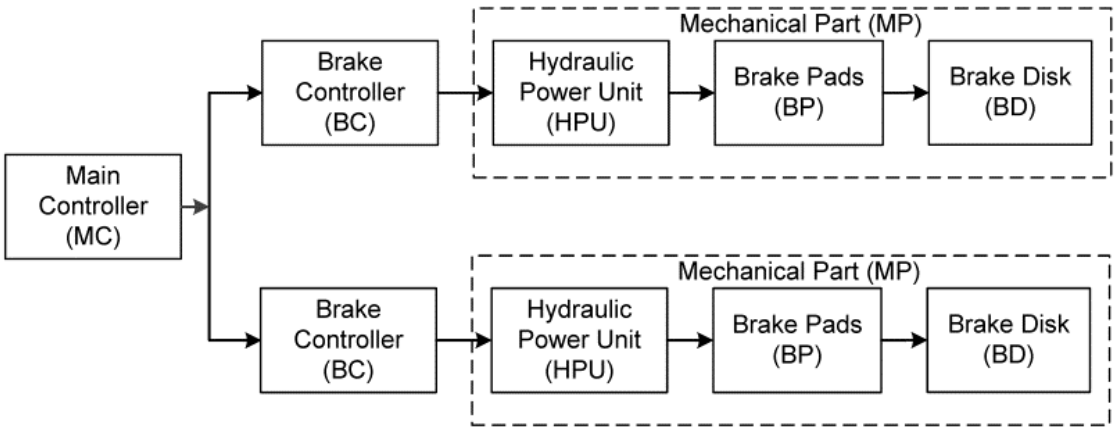

Figure 4. An example of a 1oo2 safety system architecture

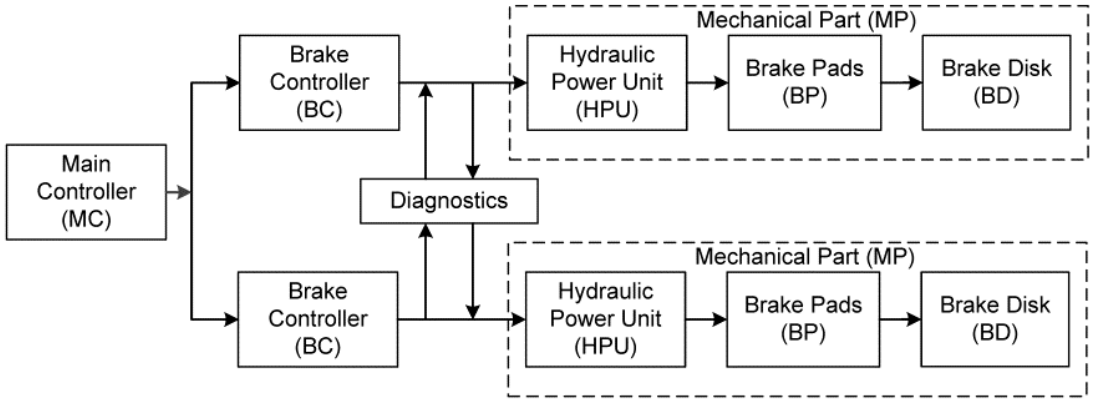

Figure 5. An example of a 1oo2D safety system architecture

With a diagnostic system, the option to detect (dangerous) failures becomes possible. The ratio, also expressed as a percentage, of the failures that can be detected is called the Diagnostic Coverage (DC). Therefore, with a diagnostic system the failure rate λ can be split in a detected dangerous failure rate per hour λ_{DD}, and an undetected dangerous failure rate per hour λ_{DU}:

$$\lambda_{DU} = \lambda(1 - DC) \qquad 5$$

$$\lambda_{DD} = \lambda DC \qquad 6$$

Some undetected failures have a common cause. The fraction of undetected failures that have a common cause is expressed as β. The Standard IEC 61508-6 provides examples of architectures and gives PFH values for different architectures and situations. In this paper, the system architecture 1oo2 and 1oo2D have been discussed. Table 6 gives an example of the probability of failure for a period of one year (τ=8,760 hours) and a mean time to reparation of eight hours (IEC 61508-6, 2010). From this table it can be learned that reliability increases when the architecture is changed from a 1oo1 to a 1oo2 architecture. Adding diagnostics

hardly has an impact for this specific configuration and operational parameters. A table like Table 6 helps to determine the required architecture in order to match the SIL of the safety system to the required SIL of the safety function. Also see Table 1. For more information refer to standard.

Architecture	DC	$\lambda=0.5.10^{-7}$		
		β=2%	β=10%	β=20%
1oo1	0 %		$2.2.10^{-4}$	
	60 %		$8.8.10^{-5}$	
	90 %		$2.2.10^{-5}$	
	99 %		$2.6.10^{-6}$	
1oo2	0 %	$4.4.10^{-6}$	$2.2.10^{-5}$	$4.4.10^{-5}$
	60 %	$1.8.10^{-6}$	$8.8.10^{-6}$	$1.8.10^{-5}$
	90 %	$4.4.10^{-7}$	$2.2.10^{-6}$	$4.4.10^{-6}$
	99 %	$4.8.10^{-8}$	$2.4.10^{-7}$	$4.8.10^{-7}$
1oo2D	0 %	$4.5.10^{-6}$	$2.2.10^{-5}$	$4.4.10^{-5}$
	60 %	$2.8.10^{-6}$	$9.8.10^{-6}$	$1.9.10^{-5}$
	90 %	$8.5.10^{-7}$	$2.6.10^{-6}$	$4.8.10^{-6}$
	99 %	$1.0.10^{-7}$	$2.8.10^{-7}$	$5.0.10^{-7}$

Table 6. Probability of failure for different safety architectures

IEC 61508-6

Example

A SIL-based method assists in the design of the safety system architecture. Table 7 shows the results of a typical decision making process. Starting from the requirement of having a SIL2 level for one year of operation of the brake without maintenance/inspection, it can be seen that a safety system without redundancy (1oo1) is not acceptable. Applying one-component redundancy improves the reliability at SIL2 level from two months to four months but is still not sufficient. After application of a diagnostics system (1oo2D), SIL2 is maintained for one year which is within the SIL requirements of the safety function and therefore acceptable.

Required SIL for a safety function: SIL2		
Safety system	**Time of exploitation**	**Achieved SIL**
1. A safety system without redundancy (1oo1)	0-2 months	SIL2
	2 months-2 years	SIL1
	for more than 2 years	no SIL
1. Decision: SIL is not appropriate (redundancy is required)		
2. A safety system with one-component redundancy	0-4 months	SIL2
	4 months -2.5 years	SIL1
	for more than 2.5 years	no SIL
2. Decision: SIL is not appropriate (to use another redundancy)		
3. A safety system with redundancy architecture (1oo2D)	0-1 year	SIL2
	1-6 years	SIL1
	for more than 6 years	no SIL
3. Decision: SIL is appropriate		

Table 7. Example of decision making for a redundancy in functional safety model

7. CONCLUSIONS AND RECOMMENDATIONS

Reliability and safety of belt conveyors is not just a scientific matter. On the contrary, it is very relevant in practice. For belt conveyors, enhancing a braking system's reliability means an improvement of its safety. Investing in additional reliability enhancing measures, and on documentation that highlights the relationship to the applicable standards has a real benefit. It is much more cost effective than saving on reliability measures and losing equipment and/or people which may lead to having to pay enormous penalties and compensations in the case of fatalities.

Despite the existence of safety standards in the belt conveyor area, there are still no functional safety standards. This paper introduced functional safety for belt conveyors, in particular for a belt conveyor braking system. This SIL-based approach presents a real measure of safety and provides a suitable tool for decision making on system architecture, redundancy, maintenance and reparation or replacement of non-functioning equipment.

Determination of a SIL helps in understanding the necessity of redundancy. The SIL of a safety system has to correspond to the SIL of the related safety function. If the SIL of a safety system is not appropriate, reliability improvement is required. In addition, the SIL can be a limit between different 'reliability zones'. An example was given that demonstrated a simplified SIL-based scheme of maintenance in two modes. This system sets a cost effective limit between SILs and predicts the time to fault (t_{per}) that allows planning reparation or replacement of equipment in advance. The SIL-based method described in this paper can also be applied to other safety related belt conveying systems. The development of a sector application standard for functional safety of belt conveyors is an interesting scientific challenge for the future and one that is required for a practical engineering implementation of the SIL-based method.

REFERENCES

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

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

3 Miguel Angel Reyes, Grant W. King & Gregory G . Miller (2014), "Intelligent Machine Guard Monitoring, A wireless system to improve miner safety", *IEEE Industry Applications Magazine,* Mar-Apr 2014.

4 Mine Safety and Health Administration Accident, Illness and Injury Database. (2001–2010). Internal analysis of conveyor guarding accidents. [Online]. Available: http://www.msha.gov/stats/Statistics.HTM

5 Rogova E. and Lodewijks, G. (2014), “Application of standards in reliability prognosis of braking system of moving walks”, ESREL 2014. In: European Safety and Reliability Conference, Proceedings, CRC Press/Balkema, Taylor and Francis Group, Reliability and Safety. Methodologies and Applications. In press.

6 Stout N A, Linn H I. (2002), “Occupational injury prevention research: progress and priorities”, *Injury Prevention* ***8,*** (Suppl. IV): iv9–iv14.

7 Hou Youfu, Xie Fangwei, Huang Fei, (2011), “Control strategy of disc braking systems for downward belt conveyors”, *Mining Science and Technology (China)* ***21,*** pp. 491–49.

8 IEC 61508-1. 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1: General requirements.

9 IEC 61508-4. 2010. Functional safety of electrical/electronic/programmable electronic safety-related system. Part 4: Definitions and abbreviations.

10 IEC 61508-5. 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 5: Examples of methods for the determination of safety integrity levels.

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

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

13 ISO/TR 14121-2. 2012. Safety of machinery - Risk assessment - Part 2: Practical guidance and examples of methods.

ABOUT THE AUTHORS

PROF GABRIEL LODEWIJKS

Prof Lodewijks studied mechanical engineering at Twente University and Delft University of Technology, The Netherlands. He obtained a master's degree in 1992 and a PhD on the dynamics of belt systems in 1996. He is president of Conveyor Experts BV, which he established in 1999. In 2000 he was appointed full professor in the department of Transport Engineering and Logistics at the Faculty of Mechanical, Maritime and Materials Engineering. In 2002 he was appointed as chairman of the department, and in 2011 became the deputy dean. His main interest is in belt conveyor technology, automation of transport systems, material engineering and dynamics.

Prof.dr.ir.Gabriel Lodewijks
Delft University of Technology
Faculty of Mechanical, Maritime and Materials Engineering
Department of Marine and Transport Technology
Mekelweg 2
2628 CD, Delft
The Netherlands
Phone : +31 15 278 8793
Fax : +31 15 278 1397
e-mail : g.lodewijks@tudelft.nl or g.lodewijks@conveyor-experts.com

ELENA ROGOVA

Elena Rogova studied at the National Research Nuclear University (Moscow Engineering Physics Institute) where she gained a specialist diploma in Automation and Electronics of Physical Facilities. She has an M.SC and is presently working towards a PhD at the Delft University of Technology, The Netherlands, in reliability and safety engineering, the project being 'Safety precautions in electrical systems'.

Her interests lie in the areas of functional safety, reliability of safety related systems and redundancy allocation, as well as in risk analysis; SIL estimation, standardisation and certification in accordance with IEC 61508 and application sector standards and automation of manufacturing process.

Elena Rogova
Mobile: +31644931705
E-mail: E.S.Rogova@tudelft.nl

..