Assessment of Safety Functions of Lignite Mining Equipment according to the requirements of Functional Safety.

Implementation of the Machinery Directive based on proven-in-use, company standards and regulations.

Dr. Thorsten Gantevoort (TÜV Rheinland Industrie Service GmbH)
Karl-Heinz Paus (RWE Power AG)

TUEV Rheinland was asked by company RWE Power to support the implementation of the Machinery Directive in Lignite Mining Equipment according to the requirements of Functional Safety.
Due to extreme dimensions and environmental conditions in the opencast mines and a wide range of company standards based on operational experience and lessons learned, an approach based on proven-in-use, company standards and regulations was used.
The analysis of the safety functions came to the result, that the quantitative parameters (PFH etc.) fulfill the requirements of the Functional Safety standards. However, the Systematic Capability of the complex components did not fulfill the requirement just by proven-in-use analysis. Therefore they had to be assessed in detailed and - as a result of the assessment - additional safety measures had to be implemented.

TUEV Rheinland was asked by company RWE Power to support the implementation of the Machinery Directive in Lignite Mining Equipment according to the requirements of Functional Safety.

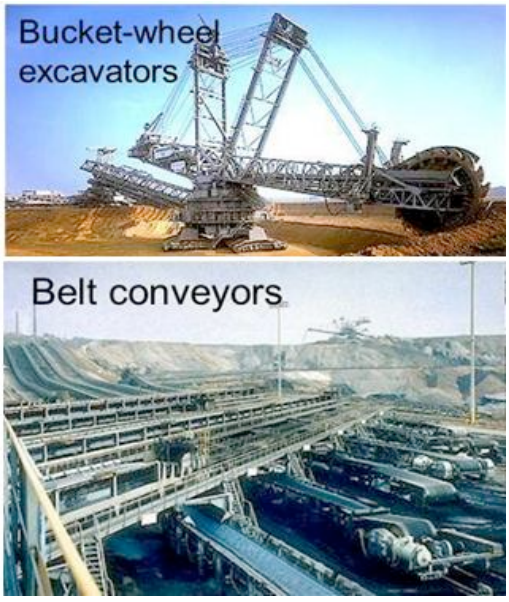

Figure 1: Mining equipment

RWE Power had already established operation standards and equipment standardization in the mining division, as the machines and equipment used in the existing dimensions are

- composed of a number of drives and functions
- operated under the most difficult environmental conditions (dust, water, vibration, etc.)
- a niche market.

Approximately 350 engineering standards with approximately 4000 pages deal with operating material (switches, contactors, cables etc.), (safety) circuits (energy, conventional circuits, PLC-circuits etc.) and procedures (documentation, construction, design for drives, functional safety etc.). They incorporate “lessons learned” since approximately 1970 as „living“ know-how collection.

Approach and method

Due to the fact that in the open cast mines of RWE Power a great number of similar safety circuits - based on the company standards - are operated over a considerable operation time, as first approach “proven-in-use” (also named as “prior use”) was applied to prove the sufficient low probability of dangerous failures according to the requirements of the standards for functional safety.

This is a common method in the process industry [2]. In the harmonized standards for safety of machinery, EN ISO 13849-1 [3] and EN 62061 [4], this method is not defined. Thus the proven-in-use method from [2] was taken and combined with the requirements of EN ISO 13849-1 [3].

The IEC 61511:2003 defines in chapter 11.5.3.2 among others the following requirements:

“*The evidence of suitability shall include the following:*

- *consideration of the manufacturer’s quality, management and configuration management systems;*
- *adequate identification and specification of the components or subsystems;*
- *demonstration of the performance of the components or subsystems in similar operating profiles and physical environments;*
- *the volume of the operating experience.”*

Around 100 safety loops were clustered and analyzed. Four typical safety loops were exemplarily selected with different PL_r requirements in order to investigate, if they can fulfill the requirements by using the proven-in-use method.

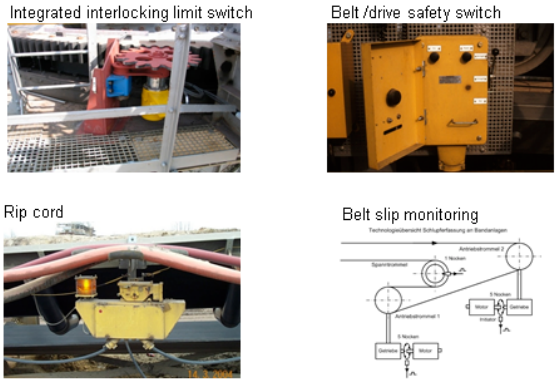

Figure 2: The four exemplary circuits

For each of the four safety circuits RWE Power provided testing and maintenance protocols as well as error and repair lists.

As the RWE Power standards require a manual testing every six month and a full testing (i.e. driving the machine such that the circuits will be activated) at least every two years a thorough and detailed database about the past experience could be established by TÜV Rheinland.

In table 1 the overall numbers of the four safety circuits are listed, which are in operation in the different open cast mines at RWE Power.

Table 1: Number of circuits

	Ham	Ind	Grz
Belt Slip Monitoring	57	43	81
Integrated inter-locking limit switch	130	45	72
Belt /drive safety switch	428	221	350
Rip cord	1462	613	727

Ham: open cast mine Hambach
Ind: open cast mine Inden
Grz: open cast mine Garzweiler

The numbers of installed safety circuits are very different for the four different types of safety circuits (see table 1). The Rip cord has in total 2802 installations and the Belt Slip Monitoring only 181.

The proven-in-use approach requires a sufficient amount of operating time. This operating time is the accumulated time of all installed and tracked installations of the same kind.

Therefore RWE Power and TÜV Rheinland had to analyze different time periods for the four safety circuits. In table 2 the evaluated operating times of the safety circuits in years per installation is shown.

Table 2: Evaluated operating time [a]

	Ham	Ind	Grz
Belt Slip Monitoring	7	2,5	4,43
Integrated inter-locking limit switch	5,85	2,47	5,64
Belt /drive safety switch	4,86	3,17	4,77
Rip cord	4,45	2,57	4,64

The operating time and the archived documentation (test protocols, error lists etc.) also vary between the three open cast mines. One reason is that in the past the safety circuits were realized differently until the company standards led to a harmonized realization.
In parallel to the data collection the safety circuits were analyzed concerning the used devices, the safety architecture and the safety function as well as the safe state. As a result the reliability block diagram and the possible category according to [3] of each subsystem was determined.
In this with paper only two of the four analyzed safety circuits are discussed, the “belt drive safety switch” and the “integrated interlocking limit switch”.
The function of the “belt drive safety switch” is to safely switch off the drives of a belt. This is initiated by manual operating an electromechanical switch, which trips a contactor. All parts of the safety circuit are low complex electromechanical devices without any software.

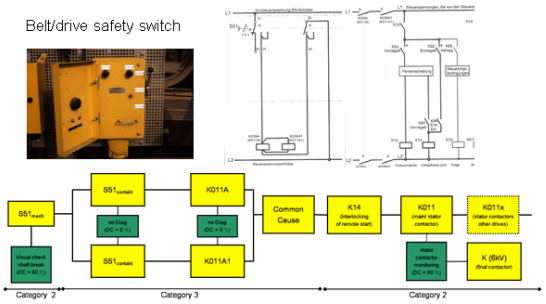

Figure 3: RBD of belt drive switch

The safety function of the belt drive safety switch was defined as: protection against unexpected start up during repair or maintenance work by safely switching off the drives.
The safe state was defined as: switched off drives.
The function of the integrated interlocking limit switch is much more complex than the function of the belt drive safety switch.
As the bucket-wheel excavators and the spreaders are big mobile machines with many axes and long cantilevers, they must be protected against collision of the cantilevers and canting over of the whole machine.

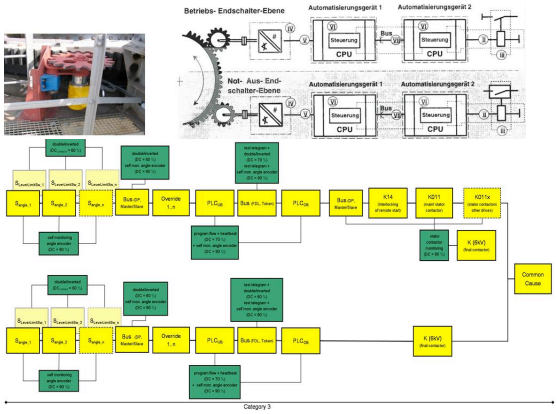

Figure 4: RBD of integrated interlocking limit switch

The safety function was defined as: protection against collision of the device with itself by monitoring the limits of the movements and switching-off the related drives by exceeding the limits

The safe state was defined as: switched off drives for the corresponding moving direction.

For this safety function many drives have to be monitored and their positions have to be transformed into the current positions of all cantilevers of the machine. The transformation is executed by standard PLCs. In addition the encoders are connected to the PLC via standard Profibus, as the dimensions are huge on such a bucket-wheel excavator or spreader.

The analysis showed that the proven-in-use method as the only approach could not sufficiently prove for this safety circuit that the PL_r could be reached. For the complex devices including firmware no sufficient information could be retrieved about the installed firmware versions during the operating period. Further on it should be possible to install new (i.e. not proven-in-use) firmware versions of the PLC in the future.

The proven-in-use approach encountered the problem that in three safety functions standard PLCs and busses were used. As a solution for this problem, a detailed assessment/analysis of the complex standard components was executed in order to develop additional measures to ensure sufficient safety.

Analysis of used PLC and results
The PLC - a Siemens S7 - was analyzed regarding random hardware faults and systematic faults including software aspects. The PLC is used in the safety functions belt slip monitoring (PL_r b), Rip Cord (PL_r c) and integrated interlocking limit switch (PL_r d).

In the safety functions with PL_r b and c the PLC is used in single configuration, in safety functions with PL_r d in redundant configuration.

The following measures for fault detection were already implemented by RWE Power according to the company standards:

- Heartbeat monitoring with external circuit
- Activation of internal sort circuit detection of I/O
- EPROM identifier for protection against mixing up application programs

The following measures for fault avoidance were already implemented by RWE Power according to the company standards:

- Change- and configuration management for hardware and application software
- Complete independent redundancy for higher safety requirements (PL_r d)
- Statement of PLC Manufacturer about firmware development based on V-Model and the use of their standard components in safety related applications

Analysis of used bus (Profibus) and results
All PLCs use the Profibus for communication.

The following measures for fault detection were already implemented by RWE Power according to the company standards:

- Complete independent redundancy for higher safety requirements (2 Profibus systems)
- Using standard measures of Profibus:
  - Even parity check
  - Checksum (Hamming Distance 4)
- Test telegram (only between PLCs)
- Consecutive number
- Angle encoder diagnosis (only between encoder and “first” PLC)

Further additional measures
The assessment of the measures implemented by RWE Power based on the company standards showed that many safety measures were already implemented. Some of these measures are specific for this application and therefore cannot be used in other (multipurpose) applications.

Nevertheless the systematic aspects of the firmware, failures in complex hardware and the residual failure rate of the bus systems were not sufficiently covered. Therefore additional safety measures were developed and implemented.

Additional measures for the bus system
As additional measure to detect bit and multi bit errors on the Profibus, the “angle encoder diagnosis” was implemented in all PLCs of the safety function.

The angle encoder diagnosis consists of four diagnoses:

- Range diagnosis
- Step interval diagnosis
- Stand still diagnosis
- Function diagnosis

The range diagnosis checks each measured – and via Profibus transmitted – value, if it fits to the general measurement range and the application (axis) specific measurements range.

The step interval diagnosis checks if the measured – and via Profibus transmitted - values are plausible concerning the continuity. It detects fluctuations (“jumps”) in the measured values.

The stand still diagnosis checks if the measured – and via Profibus transmitted - values change inadmissibly in stand still of the drive. The function diagnosis checks if the measured – and via Profibus

transmitted -values change in a given time interval, when the drive is running.
All these measures were originally developed and implemented to detected errors in cabling, the encoder itself and in software and data transmission for serial and parallel communication.
This diagnoses also support the detection of bit errors in the Profibus, as these errors will often result in implausible values, wrong step intervals etc.
The effectiveness of all applied diagnostic measures for the Profibus was checked with an FMEA based on the failure assumption of EN 61784-3 [5].

Additional measures for detection / prevention of systematic failures and failures in complex hardware
The following diagnoses cover systematic failures as well as random hardware failures:

- Using diverse redundancy (for PL d)
- Enhanced heartbeat diagnosis with program flow control on application level
- Instruction test of used instructions on application level

Diverse redundancy for safety functions with PL_r d was implemented for the standard PLCs. Diverse redundancy is a good measure against hardware and systematic (firmware) failures. As nowadays the diversity between two different devices is not always obvious, even if the devices are from different manufacturers (e. g. brand labeling is a common strategy), a statement from the manufacturer(s) is necessary about the diversity of the devices. For the safety functions at RWE Power, the diversity – especially for the firmware - between Siemens PLCs S7-400 and S7-300 was confirmed by Siemens.
However the application software (program) is not diverse. Based on the proven-in-use approach the decision was made not to create diverse (i. e. new) application programs, but to use the existing programs instead.
The application programs are exactly defined in company standards and realized in that way for many years.
Any modification has to be documented, analyzed, tested and released by defined authorities before they can be implemented. Therefore the requirements for configuration management, change and modification management are already fulfilled also.
In order to enhance the reliability of the application program as well as the firmware the additional measures program flow and instruction test were defined, developed and implemented.
The program flow control is checking the correct execution of the safety-related functions by using a counter, which is incremented in every safety-related function. At the end of each cycle the counter is compared against a target value. Only if this counter is equal to the target value, the external heartbeat circuit is triggered.
The instruction test deals mainly with systematic (firmware) and hardware failures in the PLCs. At first the used instructions for each application program were gathered. Then for each instruction an instruction test was developed and implemented.
Simplified example "testing unconditional jumps":
The value R1 is stored at a certain memory address. Executing an unconditional jump (SO1) to this address and comparing the result with a defined value R2 in the test routine.
All instruction tests are executed during runtime in each cycle.

Overall Results - Summary
The applied approach "proven-in-use" to prove the conformance of the different safety functions to the PL_r according to EN ISO 13819-1 led to good results regarding the reliability of the low complex components. The complex components like PLCs and bus system with firmware could not be assessed only with the proven-in-use approach. Especially for systematic aspects a detailed analysis had to be executed and, as a result, additional safety measures were implemented.

The so called quantitative requirements (calculation of probability of failures) were mainly proved by the proven-in-use method. In addition - as conservative approach – the probabilistic figures of the PLCs were added to the proven-in-use results. The probabilistic figures are listed in table 2 and 3.

Table 2: Results quantitative figures

	Op.Time	Demands	PFH
Belt Slip Monitoring	3,9E+06	1,8E+03	5,1E-07
Integrated inter-locking limit switch	5,8E+06	2,6E+03	1,7E-07
Belt /drive safety switch	2,0E+07	8,9E+03	1,5E-07
Rip cord	5,2E+07	2,3E+04	1,4E-06

In table 2 the PFH values (without the PFH values of the PLCs) are listed. In table 3 the PFH values of the PLCs in the respective safety functions are added.

Table 3: Results vs. requirements

	PFH_{sys}	PL_r	PFH_{Limit}
Belt Slip Monitoring	2,3E-06	PL b	< 1E-05
Integrated inter-locking limit switch	9,6E-07	PL d	< 1E-06
Belt /drive safety switch	3,9E-07	PL d	< 1E-06
Rip cord	2,4E-06	PL c	< 3E-06

As a final result of the assessment the compliance of the four safety functions with the respective PL_r could be proved for the quantitative requirements (hardware integrity) as well as for the systematic requirements (systematic integrity / systematic capability).

Outlook

The next steps of RWE Power after reaching these positive results are:

- Adaptation of the generated results into the existing company standards
- Classification and extraction of key specifications of proven operating circuits
- Verification whether the non-tested circuits comply with proven operating specifications, if necessary adaptation of the circuit
- For new circuits without proven operating, which can also not be derived from proven operating specifications, a proof of safety could be done by “classic” probabilistic evaluation (e.g. by using EN ISO 13849)

Abbreviations

PL	Performance Level
PL_r	Required Performance Level
PLC	Programmable logic controller
PFH	Probability of Failure per Hour [h^{-1}]

Dr. Thorsten Gantevoort
TÜV Rheinland Industrie Service GmbH
Am Grauen Stein, 51101 Köln
+49 221/806-4061
+49 221/806-1539
Thorsten.gantevoort@de.tuv.com
www.tuvasi.com

Karl-Heinz Paus
RWE Power AG
Frechener Strasse 12, 50226 Frechen
+49(0)2234/935-33700
+49(0)2234/935-33409
karl-heinz.Paus@rwe.com
www.rwe.com

References

[1] IEC 61508, Part 1-6:2010
Functional safety of electrical/electronic/ programmable electronic safety-related systems

[2] IEC 61511-1:2004
Functional safety –Safety instrumented systems for the process industry sector

[3] EN ISO 13849-1:2008
Safety of machinery –Safety-related parts of control systems

[4] EN 62061:2005
Safety of machinery –Functional safety of safety-related electrical, electronic and programmable electronic control systems

[5] EN 61784-3:2008
Industrial communication networks – Profiles –Part 3: Functional safety fieldbuses – General rules and profile definitions