Why PESSRAL is not PESS

Tijmen Molema

buikslotermeerplein 381, 1025XE, The Netherlands

Liftinstituut, tijmen.molema@liftinstituut.com

Keywords: PESSRAL, PESS, Safety

Abstract. The lift industry is quite old-fashioned in electric / electronic / programmable electronic (E/E/PE) safety: they used the electric safety chain for more than 30 years. However, since the EN 81-1/2 A1: 2005 amendment, the standard allows to use programmable electronics for safety systems (PESS). Also, the code committee decided to implement a subset of the leading norm (IEC 61508) into EN 81 in order to decrease the difficulty and increase the implementation speed: PESSRAL (Programmable Electronic System in Safety Related Applications for Lifts) was born. However, due to cherry picking and skipping the basics the old and even the newest code (EN-81-20/50) makes it possible to create unsafe systems. Where are the potential risks?

1 LEADING NORM

The IEC 61508 itself consists of 7 different pieces with a total of more than 500 pages. It describes the complete path to follow when creating an E/E/PE safety device. It contains calculations, assumptions, design strategies, risk analyses, and descriptions of quality systems. It results in a SIL (safety integrity level) which is a mathematical number expressing the safety of the system. All of this documentation is needed to end up in a safe system. In contrast: EN 81-20/50 uses 11 pages and claims to be a full package.

2 SYSTAMATIC CABABILITY

The entire process flow for making a PESS is described in a separate part of the standard, the 61508-1. By a clear way of working and project management we try to minimize systematic failures in a system. There are clear demands and this results in a SC (systematic capability) value. Techniques which can be used are e.g. project management, documentation, structured design and modularization as well as the SC, as these techniques are not demanded or described in EN 81-20. Projects without proper management can contain major mistakes, and these are hard to spot.

3 RISK ANALYSIS

For safety software, SIL (safety integrity level) is used to measure safety. It is a mathematical number expressing the safety of the system. For example: SIL 3 has an average chance of failure between 10^{-9} and 10^{-8} or 10^{-5} to 10^{-4} an hour depending on the demanded rate. Normally you have to perform a risk analyses in order to determine the needed SIL rate. The EN81-1/2+A3 and EN 81-20/50 have already performed this risk analyses in it and ask for SIL ratings. This way there is no need for a risk analyses anymore, which creates uniformity in the systems of competitors. However; a risk analyses gives insight in the project and influences the design. This is mandatory in IEC 61508 procedure, but not in EN 81-1/2 and EN 81-20.

4 DEMAND

So a SIL level is available, but it is not clear which SIL level we have to use exactly: the standard describes 2 types of SIL systems, high demand and low demand systems. Each of them have their own requirements. It is not clear by the EN81 if we are working in high or low demand. The difference in demand rate between these is mathematically a factor of 10.000 failures / hour. Low demand is explained in IEC 61508-4 as "where the safety function is only performed on demand, in order to transfer the EUC (Equipment under Control) into a specified safe state, and where the frequency of demands is no greater than one per year". For a lift, we do not use the over speed governor more than once a year, so is it than low demand? This is necessary to know because it gives a difference in the calculated safety by a factor of 10.000. It is not set clearly in the standard. However the IEC-62061 states that machines shall fulfill high demand. Most of the certifying organizations are following this guideline. Unfortunately it is not set plainly in the EN 81-20.

5 SAFE FAILURE FRACTION

When building a SIL 3 system, the relevant tables in EN 81-1/2+A3 and EN 81-50 require that a double channel system is mandatory. The main idea of this is 'when one channel fails, the other channel will put the system to a safe state'. IEC 61508 has the same principles, but there are some major discrepancies. IEC 61508 describes the model of SFF (Safe Failure Fraction): the fraction of failures which is safe and which is dangerous. For components where the failure mode cannot be predicted (like CPU's and other complex systems) the demands are set higher. Moreover, diagnostic software also increases the SFF. Due to the fact that EN81-20/50 demands a 2 channel system for SIL 3 it excludes the use of a totally fail-safe (SFF = 100%) 1 channel system and makes it possible to create a fail-unsafe (SFF << 90%) system. If every possible fault in a channel is directly dangerous (SFF = 0%), and if the fault remains undetected a second fault causes an unsafe system. This way, PESSRAL solutions can be less safe than the fault tree analyses present in the EN 81-20.

6 COMMON CAUSE

Due to not performing a risk analyses and the demand for 2 channels for SIL 3, a new difficulty occurs. By demanding 2 channels without any further specification it becomes possible to build 2 identical channels. These identical channels introduce the risk to fail at the same time due to the same error (common cause). Typical errors are a slightly to very low supply voltage, design faults inside a CPU, or temperature. When working with multiple channels, the common cause errors are the largest part of the total. I will demonstrate this with an example.

You can compare it with throwing a dice: by throwing a 1 you will lose: your chance of losing is exactly 1/6. To decrease this chance of losing you can add another dice, now you need two ones to lose the game. When calculating the chance of losing, we do 1/6 * 1/6 = 1/36. Now we introduce a common cause fault in this "system": a single fault which influences both channels (the dices). Due to the fact that on the other side of the dice the number "6" is represented, and for painting 6 dots we need slightly more paint. More paint means also more weight, and two opposite sides on a dice always give a total of 7. Due to this faulty design the chance of throwing a 1 is bigger than the other numbers. The chance of a double one is also bigger than the chance of another double combination. We assume that the change of throwing a 1 is 5% bigger; this value is token from the IEC-61508. The change of throwing one 1 is 1/6, a 5% higher change for one 1 is 1/6 + 1/6 * 1/20 comes to 7/40. The total change of throwing 2 times a 1 is now 7/40 * 7/40 = 49/1600, or +- 3%. As comparison, 1/36 is 2,8%.

The standard doesn't care which faults can be a common cause: all faults has to be taken into consideration as a possible common cause. Due to this, I can simplify the calculation: Take the dangerous fault and multiply it with the common cause factor. For the dices this will mean that we have the 1/6 (fault change of 1 channel) multiplied by 1/20: a factor of 1/120 is added as common cause, or 0,8%. We end up with a fault change of 2,8 + 0,8 = 3,6%. It is bigger than the full calculation, but it is on the safe side and we considered all possible common causes.

For this system the impact is still relatively small. However the fault chance of a PESS channel is a lot smaller: for example 10^{-9} Doing the same calculations, the two channel system has a chance of failing of 10^{-9}* 10^$^{-9}$ = 10^$^{-18}$. Now we calculate the common cause part: 5*10^{-2} * 10^{-9} .= 5*10^{-11} We can see clearly that the common cause part is way bigger than the single channel faults. If we have smaller failing chances in channels, than the common cause will become more important and be the dominant part of the safety calculations, as well as they are in real safety. EN 81 does not tackle this problem: the common cause risk is not described, there are no techniques for common cause avoidance described, and nothing is calculated.

7 DIAGNOSTIC TECHNIQUES

EN 81-20 cherry picks a number of techniques and states them as mandatory. There is no calculation needed anymore (EN 81-50 states that IEC 61508-6, which explains the calculations, is not needed for understanding). IEC 61508 gives a large number of options; the most suitable technique can be chosen for the system. It can happen that completely non-relevant techniques are demanded, where other techniques are quite more useful. For example; there are no demands for sensors in the lift standard, but when we use a CLPD (complex logic programmable device) there are still demands for RAM checks and watchdogs; this is not right according IEC 61508. Also, we cannot check if our diagnostics are good enough. Normally DC (diagnostic coverage) has a direct influence on the SFF (safe failure fraction), and so on the entire safety calculation of the system.

8 CALCULATIONS

The backbone of IEC 61508 are the underlying calculations. By looking at all components FIT (failure in time) rates and design, a calculation of the chance of failure can be made. The calculated numbers should be in line with the SIL rate. FMEA (Failure Mode Effect Analyses) on components and DC in order to improve the SFF ends up in a safer system. IEC 61508 has demands on the SFF which needs to be met. The calculation is the theoretical basis, it gives insight in the weakest points of the system and proves that the system is safe enough. This calculation is not needed for EN 81, by fulfilling all demands you are done. These demands describe techniques only, but does not give any numbers. There is no check if the system is “safe enough”. It is possible to end up with a mathematical unsafe system.

For example: I can use two really bad relays parallel. When they fail once in every 10 times, they will both fail at the same time every 100 times (excluding common cause!). It still fulfills EN81-20 (double channel with diagnostics): I can detect that both relays are failing. However: I cannot act on it anymore. When we calculate the failure rates for the system with IEC 61508, we will directly find out that the relays are not good enough for this system: the FIT (failure in time) values will be devastating for the PFH (Product Failure / Hour). Due to the calculation, bad components are filtered out.

9 TESTING

Every system needs testing after development: there are always unforeseen problems which are filtered out during the test phase. Of course a PESSRAL system will be tested, but what test strategy is the proper one? Known that most of the industry has no practical experience with safety software and there are no test strategies mandatory or even mentioned in the standard. Most commonly known test method is black- / white box testing: it is a basic way of screening a system. It is usable for electric- and mechanical systems. When creating PESS, the system is a full black box: However, IEC 61508 can also ask for traceability of the requirements, full modeling, software simulation and performance testing. Also there is no test procedure or awareness for common cause faults in the lift norm.

10 PROOF TEST INTERVAL

The lifetime of a system is not considered. Due to the fact that periodical inspection on PESS systems is almost impossible, a lifetime must be specified. Diagnostics in the system also cannot detect every possible fault, the DC is always smaller than 100%. Normally PESS systems have a “proof test interval”. The meaning of this proof test is to detect the normally undetected errors. EN 81 does not require this. This allows a system to build up an endless amount of errors and gives the possibility to end up with a dangerous fault.

11 DISCUSSION

At this moment, only a small amount of lifts work with PESS. For the ones that work, there are no major failures yet. PESS is possible since the first amendment of EN 81-1/2 in 2005. We do not know how many installations are in the field today, so we cannot determine why there were no failures. There are some possible explanations that can explain the fact that we did not have any accidents:

1. When making something revolutionary, a company must be absolutely sure that it is safe: otherwise the product will not be accepted in the market by the costumer. For PESSRAL, most lift company’s want to be absolutely sure that after several years it still works: so endurance tests will probably be done. This is a powerful testing method.
2. There are not that much PESSRAL systems in the world: most lifts have a long lifetime and controls are not regularly changed. Also the development of PESSRAL has just started: there are not that much PESSRAL systems on the market. Most of them are still in development.
3. The major certification bodies also perform tests on PESS systems. They have their own demands for testing, or will ask for a calculation. Certification bodies also want safe systems, and most of them know how to perform the tests properly due to the experience with IEC 61508.
4. There is no guideline for reporting crashes, and we cannot be sure that we will hear about all crashes in the world including the cause.

The biggest problems of these possible explanations are the fact that they are not mandatory: there are no demands on test time, there is no requirement for experience in PESS for notified bodies. Also worldwide information about lift catastrophes does not exists related to this topic.

12 CONCLUSION

PESSRAL is not PESS: and this is not only due the absence of a lot of background information. The entire mathematical backbone is gone: we cannot calculate if the chance of failure of the system is right. This has a huge impact on the common cause faults. These are the most dangerous faults for a double channel system. Also the channels itself can be made out of unsafe components. The only way to check the system now is by testing, but testing strategies are not described. Until this moment of writing, there are no fatal accidents yet. However we cannot explain why they did not happen, or predict that they will not happen. In the end, it is possible to build unsafe systems with the rules of PESSRAL. For now we can only hope that lifts will stay safe, for the future we need EN 81-20 to change as quickly as possible.

BIOGRAPHICAL DETAILS

Tijmen Molema is a product specialist certification for Liftinstituut. His specialty is in software and electronics. He studied Electronic Engineering and Design at the Hogeschool Utrecht. He started in 2014 as a lift inspector, but quickly became a product specialist for all kind of electronic challenges.

His personal goal is to help the lift industry to leave the “old” relays systems, and lead it to a new and progressive market.

Liftinstituut is an independent Body which is specialized in product certification and surveys of hoisting equipment for goods and persons. Liftinstituut is therefore also notified by the Dutch authorities as Notified Body(0400) for the Lift directive (95/16/EC) and machine directive (2006/42/EC) for e.g. *lifting devices of persons or of persons and goods involving a hazard of falling from a vertical height of more than three meters hoisting and logic controllers.*

In the USA Liftinstituut is also registered as AECO for Lifts (0842).