

Cost of Safety in the Process Industry

Kees Kemps,
Director Sales & Marketing,
Honeywell Safety Management Systems
PO Box 116
5201 AC 's-Hertogenbosch

Keywords:

Fault Management, S-84.01, dIEC-61508, Diagnostic based technology, Peopleware, Quality Systems on Safety, Overall Safety Lifecycle.

Objectives and perceptions

All companies have clearly defined goals for their business and have addressed most values and variables within their operations. Safety has become an important topic for all companies. Qualification and quantification of safety are an ongoing process in daily management. Changing the wording in order to increase the awareness allows us to communicate about “profit of risk” rather than “cost of safety”. There is a given relation between safety, faults and risks as there is one between cost and profit.

Many companies have invested heavily in safety measures within their operation in an attempt to address the issues that contributed the most. History has taught that many investments have been incorrectly addressed.

Most companies approach the safety issue from the cost perspective; all investments, both capital expenditures (CapEx) and operational expenditures (OpEx), have been reduced where possible, without clear definition of the level of safety/faults/risk. If, in an equation, one side is not clearly quantified, the entire equation loses its value, and the implementation of the measures based on the conclusions from this approach becomes an unmanageable task for management.

This is the main topic addressed in the emerging standards, both the US-ISA standards on safety S-84.01 and the international standard dIEC-61508. Both standards clearly address the risk assessment side of the equation as well as the investment side by addressing the technical solutions available today. Both standards deal with the cost issues during the entire life time of the operation, considering both CapEx and OpEx as an integral part of the Overall Safety Life Cycle Costs.

Fault Management

The title of the IEC-61508 is “Functional Safety”. In order to maintain the functionality of an entity, one has to concentrate on faults that can affect the (intended) functionality. Both standards describe various measures to avoid or prevent failures from occurring as well as measures to detect failures, and they describe methods to isolate the negative impact of failures. The diagram below clearly illustrates the intention of the standards: it is aimed to act as an “umbrella” for failures that can influence the functionality.

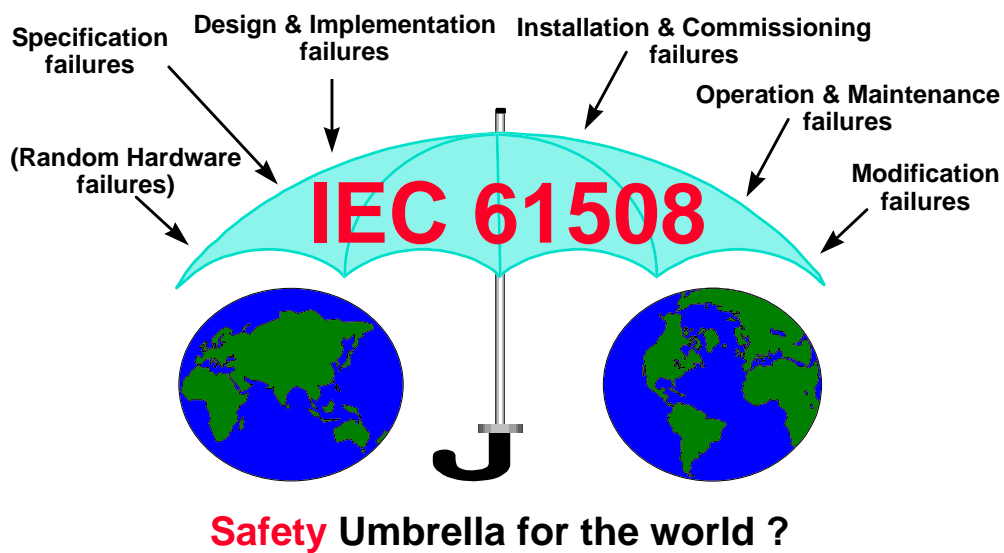


Figure 1 Overview of Possible Influences on a Safe Operation.

In addition to the (random) failures within hardware and (systematic) failures within software, Figure 1 addresses the errors, mistakes, omissions made by **peopleware**. Studies have shown that less than 10% of failure causes is related to hardware, whereas software and peopleware make up the remaining 90%. With this in mind, it is not surprising that most recommendations contained in both standards focus on quality measures on safety that should be implemented in both the vendor's and the user's organizations.

Lessons learned

Field returns are the ultimate proof of predictions made during the initial design. Considering several accidents (negative experiences) over recent decades, the unfortunate conclusion must be that the “cost of safety has indeed been incorrectly validated by peopleware and has ultimately had a negative impact on the defined objectives.

Example 1

NASA’s Space Shuttle program was started in the late seventies. Risks analyses were carried out for the shuttle design, and risk calculations showed figures varying between “1 in 100” and “1 in 100,000” launch operations. The design was ultimately approved as adequate, and the construction was started. The first shuttle was launched in 1981 and many successes would follow.

During the reassembly works of the solid fuel booster rockets it was discovered that problems could arise with the seals between units manufactured and assembled in various states within the US. Problem reports initiated by the assembly engineers were ignored by management over several years until 1985, when they finally reached the management level. Investigations for improvements subsequently initiated. The recommended improvements would delay the launch program (impact on profit and image), and the costs were estimated at USD 500 million.

Just before the improvement program was approved, the launch of the 25th Shuttle, the Challenger, was scheduled to bring seven persons into space. Normally, only five persons would be carried by the Shuttle, but in order to boost the program’s image, it was decided to add two “non-engineers” to the crew, to show that the Space Shuttle program was safe. The decision was made to go ahead with the conventional outfit, led to the catastrophic accident with the Challenger which killed all seven astronauts. Investigations later showed that the accident had been caused by a number of factors including faulty seals and extremely low temperatures at launch time.

The result was a three-year delay of the Space Shuttle launch program, and overall costs of redesign and operational losses amounted to a total of USD 3 billion.

Conclusions:

- What is the reliability if calculated risks differ by a factor 1000?
- There was a lot of ignorance from management on reported problems (peopleware, mismanagement).
- OpEx costs of safety improvement *after* the accident turned out to be 600% of CapEx.
- The image of the Space Shuttle program had been badly damaged.
- And, of course, there had been seven fatalities.

Example 2

In the Netherlands, Shell decided to a major refurbishment of their Pernis refinery located in Europoort, close to Rotterdam. Entire process units were renewed, including the process equipment that was over forty years old. The total investment in this “Per+ Project” amounted to USD 1.7 billion.

Risk assessments and Instrumented Protective Function (IPF) classifications were made, and the overall investment in process control and process safeguarding was USD 60 million (CapEx).

After three years of operation, a study was conducted into the operational expenditures (OpEx), which resulted in USD 10 million per year for depreciation, costs of maintenance and testing, costs of nuisance trips and an estimated amount of costs for dangerous trips.

Conclusion:

After three years of safe operation the concept that was implemented has proven it fully meets the expectations, and the OpEx costs appear to be only 0.6% of the overall CapEx. According to Shell, “good safety can be good business”.

Most Significant (Negative) Contributor to Risk/Safety/Profit.

Despite both qualitative and quantitative measures as proposed within the standards, ultimately we are left still with following failure causes which require actions during the entire life time of the operation.

Hardware failures:

- Systematic failures, like design failures.
- Random hardware failures.

Software failures:

- Software failures are only systematic failures. The failure is (unintentionally) “designed-in” into the system software and/or applicable software.

Peopleware:

- Failures can occur due to the nature of human beings.

Systematic failures can be addressed by qualitative measures (ISO, TickIt, etc.). Field returns will show whether the implemented measures will be sufficient.

Hardware Failures

Random failures within hardware can be found by periodical testing within “off-line proof test interval”, as it is called in the standards. This requires maintenance staff, with all the associated costs. Depending of the quality of testing and the “reliability” of peopleware, the random failures may be found and corrected.

It should be noted that manual testing turns the hardware problem into a peopleware problem, that in practice has turned out to be the worst of all options!

Diagnostic based technology that is available today allows “on-line testing” without any persons being actively involved. If “on-line testing” is carried out within the “fault tolerant time of the Equipment Under Control (EUC)” or within the “Process Safety Time (PST)” the overall solution results in an inherent safe solution.

Safety technology available today allows for diagnostics to be executed within this process critical time interval.

Software Failures

Vendors of safeguarding systems need to take adequate measures during the research and development stage of the safety related system so as to minimize any system software anomalies.

Users and/or system integrators of safeguarding systems need to ensure the correctness of the application software by adequate testing (peopleware).

Here too, it should be noted that manual testing turns the software problem into a peopleware, which in practice has turned out to be the worst of all options.

Vendors of safety related systems need to provide tools as integral part of their system concept. These should support functions that uncover possible failures that were introduced during the design of the application software.

Verification tools and revision control tools, utilizing a diversity of software programs, can significantly reduce the possible failure causes during the design and translation of the application software.

Peopleware issue

As stated before approximately 90% of failures are caused by peopleware. This calls for a comprehensive “quality on safety” assurance system or calls for safety management systems.

It should be noted that adding more staff to address this issue will only increase the amount of peopleware, and therefore the level of risk.

Clearly defined responsibilities, tasks and planning require discipline to be implemented at all levels within the operation.

Where possible the software tools supported within the safety concept should relieve peopleware in their tasks, ultimately resulting in a “fail safe concept” or in a “fail safe colleague”.

Conclusions

Diagnostic-based hardware technology with supportive software tools is available today, which means we can really challenge the “most unreliable factor in safety land”. A safety concept that includes hardware testing and the use of proven software can greatly reduce the contribution of peopleware to risk. This is done by putting disciplines in place which challenge people in an objective and supportive manner.

References:

- IEC-61508 1998
 Functional Safety of E/E/PES safety related systems
- ISA S-84.01 1996
 Application of Safety Instrumented Systems for the Process Industries
- DIN V VDE-0801 A1 1994
 Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben.