Session Two:

Top 10 Failures and How They Can Be Avoided

Tino Vande Capelle
Director - Functional Safety Consultancy Services
HIMA Australia Pty Ltd

Abstract

Major accidents like Seveso, Flixborough, Piper Alpha, Bhopal, Chernobyl, Texas City, and the most recent Deepwater Horizon have painfully revealed failures that we can learn from. Human nature does not like to admit or reveal knowledge of problems and therefore people still remain the weakest link in the safety culture. Competency of every person working in the lifecycle of our process industry, is becoming the 'de facto standard' for those who want to keep their plant safe, productive and avoid very costly penalties and lawsuits. The author will draw on his 30+years experience to give the audience the top 10 most common failures and how they can be avoided.

Introduction

Why is it so difficult to learn from mistakes others have made in our industry? Would you rather learn from the mistakes of others or make them all yourself? Certainly, you will learn better by making your own mistakes, but those lessons can come with extreme high risk and cost.

There have been several unfortunate industrial disasters in the process industry in the past. There will likely be many more to follow as our daily working conditions, materials, equipment and performances keep changing and getting more and more demanding. Major accidents like Seveso, Flixborough, Piper Alpha, Bhopal, Chernobyl, Texas City, and the most recent Deepwater Horizon have all painfully revealed certain failures that we can learn from. Failures that come with a cost of life, environment and capital investment.

Today, we have the knowledge that each of them could have been prevented if people would have designed the plant or process for failure and used adequate competency to avoid such things happening again in the future. But as Mr. T. Kletz (2009) once stated: "Accidents are not due to lack of knowledge but failure to use the knowledge we have."

Human nature does not like to admit or reveal knowledge of problems. So for the past 30 y, certain standards have helped engineers apply good engineering practices, but the weakest link in the safety culture remains the human being. Standards such as, but not limited to, DIN V 19250 (1989), ANSI/ISA 84.01 (1996) and the later ANSI/ISA 84.00.01 (2004), EN IEC 61508 (1998) and the later EN IEC 61508 Edition 2.0 (2010) and EN IEC 61511 (2003) have been put

in place to encourage a safety culture in our industry in the hopes of achieving a better world where people, environment and investment can be safe.
The objective of this paper is to begin with a short overview of some of the major accidents followed by a discussion on how these accidents have influenced the safety standards and culture. New technologies have initiated some of those Functional Safety Standards to bring out revisions. Edition 2.0 of the EN IEC 61508 (2010) has been released since April 2010 and has some significant changes.

In closing, in order to achieve the adequate safety culture, competency of every human working in the lifecycle of our process industry is becoming the 'de facto standard' for those who want to keep their plant safe, productive and avoid very costly penalties and lawsuits if things go wrong like in the past have been proven. Over the last 7 years, the author has been training worldwide +1500 people under the competency review program from TÜV Rheinland and will give a summary of the top 10 most common failures found among all classes.

1. Modern history of disasters

There have been several unfortunate industrial disasters in the process industry in the past. In Europe in the seventies, some of the disasters were the initiators of investigation that led to the start of guidelines and directives to achieve process safety and try to avoid similar accidents in the future. The below summary is just a glimpse of a few disasters that changed the process safety culture.

On the 1 June 1974, at a chemical plant based in the United Kingdom called Flixborough, during some maintenance, a temporary bypass pipe rupture between reactors caused a, explosion equivalent to 15 tonnes TNT, killed 18 employees in the control room, 9 other site workers and 1 cab driver died from a heart attack. Observers have said that had the explosion occurred on a weekday it is likely that more than 500 plant employees would have been killed. Resulting fires raged in the area for over 10 d. The bypass pipe failure was due to design shortcomings from personnel who were not experienced in high-pressure pipe work. It was Britain's biggest peacetime explosion until the Buncefield Depot explosion in 2005.

On the 10 July 1976, another explosion in a chemical plant Meda, known as Seveso, 15 km north of Milan causing a dioxin crisis, toxic cloud (TCDD) release in atmosphere, evacuation of the Seveso community (17,000 people) and about another 100,000 people in other neighbouring communities. About 3,300 animals died in days, and another 80,000 slaughtered. 447 people from 1,600 examined suffered from chloracne, 26 pregnant women opted for abortion. This accident has resulted in a Seveso II directive that is today mandatory; the directive aims at the prevention of major-accident hazards involving dangerous substances. Secondly, as accidents do continue to occur, the directive aims at the limitation of the consequences of such accidents not only for man (safety and health aspects) but also for the environment.

On the 2-3 December 1984, Bhopal, Union Carbide India. By far one of the world's worst industrial disaster, and the hope has to be that we never have something similar in the future. A runaway reaction in a tank generated a major temperature increase, resulting in venting/releasing 41 tons of deadly methyl isocyanate gas, killed between 3,000 – 5,000 people in the first days, until today more than 25,000 people died because of the gas leak. None of the 6 safety systems/layers were working and evacuation plan did not exist.

On the 6 July 1988, Piper Alpha, situated on the Piper oil field, approximately 193 km northeast of Aberdeen-Scotland, was originally designed as an oil platform and then later converted to gas production. An explosion and the resulting oil and gas fires destroyed it on 6 July 1988, killing 167 men with only 61 survivors. The disaster was based on an accumulation of errors and questionable decisions. Most of them were rooted in the organization, its structure, procedures, and lack of safety culture.
The above disasters led to many investigations and publications, all of them had human failure and culture as one of the main reasons 'WHY' things can go wrong. Most disasters that followed after the above events confirm that: "Accidents are not due to lack of knowledge but failure to use the knowledge we have" (Mr Kletz,2009).

Accidents such as but not limited to: 23 March 2005 - Texas City USA - BP refinery explosion - 15 killed – 170 injured # 11 December 2005 – Hemel Hempstead U.K. – Buncefield Oil storage depot explosion and fire - 43 injured – 2000 evacuated # 20 April 2010 – Deepwater Horizon – Gulf of Mexico – BP Rig explosion and fire – 11 killed – 17 injured – spilled about 780 million liters of hydrocarbon continuing for 87 days causing a massive environmental pollution…

The HSE (Health and Safety Executive) a U.K. based independent regulator acting in the public interest to reduce work-related death and serious injury across Great Britain's workplaces has published a small pocket book called "Out of control: why control systems go wrong and how to prevent failure". In summary, the HSE analyzed 34 incidents and came to the shocking conclusion that 44 % of all failures were designed to go wrong from day 1. The other failures that contributed to the disasters were 15 % design and implementation, 6 % installations and commissioning, 15 % operations and maintenance and 20 % changes after commissioning.

But bad things keep happening since systems aren't perfect; stuff (will go) goes wrong. We need to design for failure!

2. Functional safety standards and norms

'Safety' was in the older days achievable as long people used a 'safety system'. In 1984, the TUV released a handbook "microcomputers in safety technique" to help developers and manufacturers designing safety systems; shortly followed by the requirement classes (RC) specified in the DIN V 19250 standard. Not before the first Safety Lifecycle approach with Safety Integrity Level definitions specified in the EN IEC 61508 and the later EN IEC 61511 we changed from 'Safety' to 'Functional Safety'. From then onwards, good engineering practices are there to help the engineers to design, maintain and operate safety system 'Safe' and to achieve the ultimate process safety in able to protect them against the residual risk. But both the EN IEC 61508 and EN IEC 61511 are performance oriented standards, not prescriptive.

Safety systems and instrumentation used nowadays are getting more and more reliable, however the weakest link remains the 'role' of the human contribution in the safety chain. The human factor or weaknesses can be categorized as systematic failures and have specific measurements and methods described in the functional safety standards on how to avoid those potential failures.

3. Human error and Key Performance Indicators (KPI)

As mentioned above, every accident investigation shows that it is seldom 1 single instrument failure that leads to the disaster; usually it will be a combination of random hardware-, common cause hardware- and systematic-failures that will contribute in different proportion depending from case to case. One thing for sure, there will always be a large part of human mistakes/shortcomings defeating the process safety layer. Before organizations depend on the quality of a human intervention, they better make sure that the anticipated action will be reliable and help them to prevent disaster from happening.

In the safety world we can try to implement better or reliable instrumentation and systems using redundancy and diversity. But how about the operator, maintenance engineer, management etc, how do we ensure that we have adequate competency that will help us achieving the necessary process safety level?

We have probably all heard some variation of the following quotes: "You get what you inspect, NOT what you expect" or "You don't improve what you don't measure", very simple quotes with so much truth in it, therefore we all understand the importance of performance indicators that will help us achieving process safety. There have been in the last couple of years worldwide a lot of initiatives releasing public documents that define leading and lagging indicators enabling process safety performance improvements. (see references below at the end of this paper). However, "listing human error as one of the causes of an accident is about as helpful as listing gravity as the cause of a fall" (Mr. Kletz,1993). Although we may have many literatures, Key Performance Indicators remains a challenge for most organizations to understand, apply and control.

Some examples of potential KPI's:

Employee Participation	Process Safety Information
Process Hazard Analysis	Operating Procedures
Training / Competency	Compliance Audits
Trade Secrets	Mechanical Integrity
Hot Work Permits	Management of Change
Incident Investigation	Contractors
Pre-Startup Safety Reviews	Emergency Planning and Response

Only with a strong safety culture and the support of management driving the competency and controlling the measurements with a calibrated approach minimizing subjectivity could help organization avoiding major accidents happening in the future.

4. Competency and training

With the release of the good engineering practices standards like EN IEC61511 (2003) for achieving functional safety (FS) in the process industry, many different cultures, languages and interpretation has led to many different approaches of how to comply to the leading FS standards. Very often the 'safety' numbers and reports (SIL, PFDavg etc) are pulling a screen in front of the engineers eyes forgetting the 'common sense' or better say getting lost in the jungle of functional safety definitions.

The challenges for process safety implementation is not getting easier, due to:

- Increasing complexity of process operations, process control and safeguarding equipment are more complex, thereby increasing newer risks.
- Furthermore failure of multiple layers of protection, or a series of events to lead to major incidents
- Poor management, lack of awareness, lack of competency, limited focus on optimizing production.
- Ineffective communication between the plant workers and the management
- Technology transfer from the western world to countries with different culture and standardization of standards.
- Loss of process specific experience or competency due to job hopping or retirement of key personnel

Therefore competency and a proper training strategy can only enhance the achievement of the necessary process safety layer. Since the release of the EN IEC 61508 ed. 2.0 (April 2012), 'competency' has become a 'normative' requirement. There have been several competency review schemes released in the past 12 years, CFSE (2000), TUV FS Eng (2004), ISA training (2008), TUV FS for SIS professionals (2008). One of the current leading program

started in 2004 is from TUV Rheinland, trained and certified +6100 engineers (status Dec 2012) worldwide and is still exponentially growing, is proving that the market is slowly understanding the importance of having competent people helping them in the safety lifecycle achieving the adequate process safety level.

5. Top 10 failures that jeopardise functional safety based on experiences

The following summary is purely based on first hand experiences from more than 20 years conducting safety seminars, workshops and trainings, meeting thousands of people from all continents of the world, summarised in a TOP 10 collection of typical failures often found in daily discussion with safety class participants

1. Hazard identification

The most crucial phase in the life cycle for any project and yet so many companies use HAZOP methodology as a formality. It should be the first and most important step when identifying the required safety functions for your safety instrumented system (SIS). A safety function is useless when it cannot be linked to a hazard or hazardous event. Thinking about the unthinkable or outside the box is a challenge for all hazard risk analysis (HRA) teams. Keeping the brainpower time within maximum 4-6 hours and have a maximum of 8 most experienced engineers can be an asset for a successful hazard identification exercise. Last small hint, take all HAZOP reports and have the auditor checking ‘proof of evidence’ (documentation) that ALL ‘required actions’ from during the HAZOP exercise have been implemented, tested, verified, assessed and documented.

2. Risk reduction tools

Many companies are using risk reduction tools like risk matrix, risk graph, lopa etc. without calibrating the tools, because maybe corporate office defined the criteria, or the EPC contractor / consultant has proposed their preference. Whatever tool you decide to use, make sure that: 1. You calibrate the tool(s) first to your specific needs, criteria, environment, projects and plant specifics. 2. You don’t accept just cut-copy-paste between projects. 3. You periodically review (e.g. yearly) your tools and recalibrate them if needed.

3. Layer of protection analysis(LOPA)

LOPA is an ideal tool to play with numbers; this is probably why so many companies like to use it. However make sure that ALL layers are completely independent of the initiating event of other layers; therefore you can only take once credit for a layer in LOPA. Any combination of normal PLC or DCS/BPCS interlocks are maximum Risk Reduction Factor <= 10 (SIL 0). Beware of common design (systematic) failures.

4. SIL and PFD

There is this misunderstanding that with both a Safety Integrity Level (SIL) and Probability to Fail on Demand average (PFDavg) number you can express safety achieved for your safety instrumented functions (SIF). But those SIL and PFD are only a small part of the technical requirements. What is very often forgotten are the management or non-technical requirements of the functional safety (FS) standard(s). Applying a good FS management strategy can help you to avoid systematic failures and supervise competency, assessments and audits.

5. SIS and complete loop concept

Simply speaking, many safety instrumented functions (SIF) are being build using a combination of different technology, different manufactures etc. Beware that the weakest link can take down the complete safety integrity of that SIF. Example: it doesn't make sense to use a safety related output module to drive a non-safe interposing relay. Every single subsystem should fulfill the SIL requirements.

6. Proof test coverage and frequency

There are some SIL calculation (software) programs on the market to calculate the achieved SIL per SIF that have the default proof test coverage as high as 90%. There are even companies who believe that they achieve 80-90 % coverage during the periodic required SIF functionality test. Not ONLY the Frequency (how often) you will test your functions is important to follow BUT even more important is the achievable coverage of the safety functionality. Example is given in the below Figures 6a and 6b. Even when you keep the frequency of 6 months the same, a coverage of 50 % (Figure 6b) will lose or decrease the achievable SIL level after exactly 18 months. Simplified to remember: It doesn't matter how often you go visit a doctor for a medical check up, make sure that your doctor will find all potential problems, have all the required equipment to have the maximum coverage of your medical status. That is the same with your instrumentation, and systems, it doesn't matter how often you proof test them, but how will you prove the achieved coverage of the safety function?

Figure 6a shows a theoretical proof test interval of 6 months with a 100 % proof test coverage.

Figure 6b shows a theoretical proof test interval of 6 months with a 50 % proof test coverage

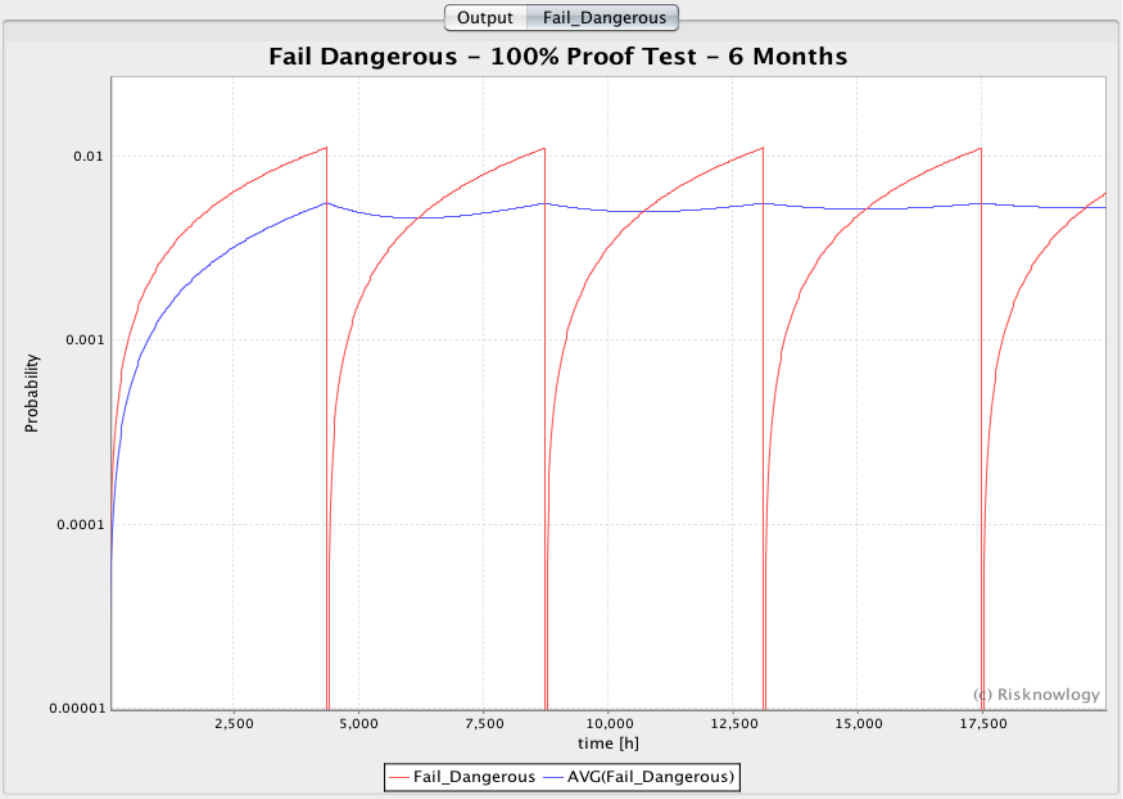

Figure 6a

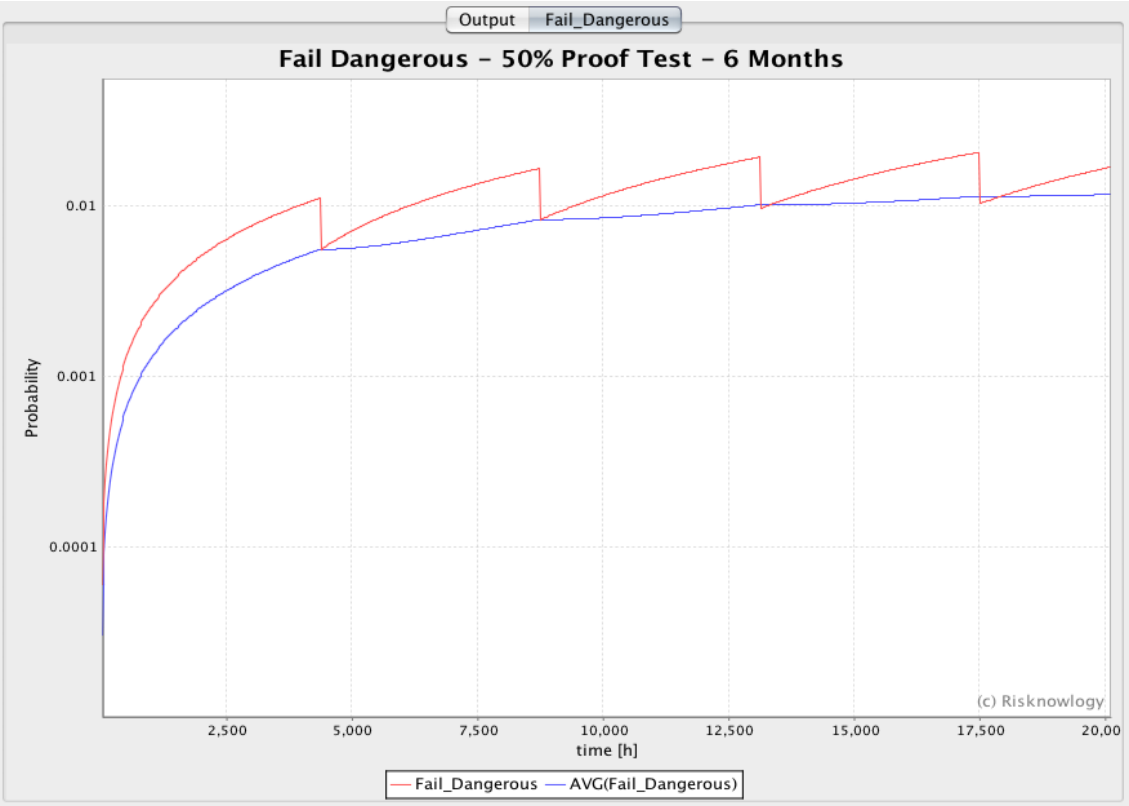

Figure 6b

7. Hardware with implemented software, SIL by FMEA?

There are numerous of field devices installed in the plant that have software incorporated in order to achieve the functionality of that device (think about field transmitter, they all have software onboard nowadays) Some of them have used only a FMEA to predict the achievable SIL level of that device. However, many times software has not been checked, nor verified. But even when you would have a full software and hardware compliant device, it doesn't necessarily achieve a higher SIL level by putting 2 together in a 1oo2 configuration because of software design limitation.

8. Certificates-reports and safety manuals

It is unbelievable how many people have never read in detail a certificate that should come (sometimes) with a safety device/system other than the magical SILx number. Mostly a report, when provided, is never looked at, however the report should explain the user of how the certificate (SIL level) was achieved and what the potential restrictions are (if any). Furthermore the EN IEC61508 ed2.0 is also requesting a Safety Manual, where the manufacture has to explain the end user how to install, commission, operate, maintain, repair the device in able to comply to the SIL level. Summary do not buy a product unless you receive a certificate + certificate report + product specific safety manual, once received read what the documentation is trying to tell you!

9. Safety availability versus Process availability

This is probably one of the oldest and biggest misunderstandings in the process industry. To be clear the FS standards don't care about process availability, they only handle safety availability by predicting potential 'dangerous failures'. Only the end-user / management care off-course also about process availability, spurious trip caused by 'safe' failures.

Please refer to the case study (Moon-HFT table) at the end of the session

10. The jungle of Functional Safety

Functional Safety standards are not black and white or cast in stone; they are performance-oriented standards, not prescriptive. The standards are open for interpretation; they are also just as prone to be open to misinterpretation and that off course has transferred the safety market in a jungle of functional safety documentation, definition, concepts etc.

6. Conclusion

The purpose of this paper was based on a short overview of some of the major accidents followed by a discussion on how these accidents have influenced the safety standards and culture; that nevertheless history of mistakes leading to disasters keeps on repeating despite all guidelines, standards and recommendations. Avoiding human failures using KPI's together with competency has to be considered in the hope of minimizing history repeating again in the very near future.

References

- DIN V 19250, Fundamental safety aspects for measurements and control equipment, (Germany,1989)
- ANSI/ISA 84.01, Application of Safety Instrumented Systems for the Process Industries, (US,1996),
- ANSI/ISA 84.00.01, Functional Safety: Safety Instrumented Systems for the Process Industry Sector, (US, 2004)
- EN IEC 61508, Functional Safety of electrical/electronic/programmable electronic safety-related systems, (Europe,1998)
- EN IEC 61508 Edition 2.0, Functional Safety of electrical/electronic/programmable electronic safety-related systems, (Europe, 2010)
- EN IEC 61511, Functional Safety: Safety Instrumented Systems for the Process Industry Sector, (Europe, 2003)
- CCPS (Center for Chemical Process Safety) – AIChE (American Institute of Chemical Engineers), Process Safety Leading and Lagging Metrics (2008)
- OECD (Organisation for Economic Co-operation and Development), Guidance on developing Safety Performance Indicators (2008)
- OGP (International Association of Oil & Gas Producers), Process Safety – recommended practice on Key Performance Indicators, report No. 456 (2011)
- HSE-UK (Health and Safety Executive, United Kingdom), Developing process safety indicators HSG254, ISBN 978 0 7176 6180 0 (2006)
- HSE-UK (Health and Safety Executive, United Kingdom), Out of control: Why control systems go wrong and how to prevent failure? (2nd edition) ISBN 0-7176-2192-8 (2003)
- CCPS (Center for Chemical Process Safety) – AIChE (American Institute of Chemical Engineers), Layer of Protection Analysis, simplified process risk assessment ISBN 0-8169-0811-7 (2001)
- CCPS (Center for Chemical Process Safety) – AIChE (American Institute of Chemical Engineers), Guidelines for Safe and Reliable Instrumented Protective Systems ISBN 978-0-471-97940-1 (2007)
- IChemE–UK ((Institution of Chemical Engineers, United Kingdom), HAZOP, Guide to best practice, ISBN 978-0-85295-525-3 (2008)
- HIMA Italia safety road show presentation, “HIMA FSCS - Why is it so difficult to learn from someone else’s mistakes - rev 02” T. Vande Capelle - HIMA Paul Hildebrandt GmbH + Co KG (2012)
- White paper, Functional Safety: Guiding principles for End-Users and System Integrators, Dr. M.J.M Houtermans – Risknowlogy, T. Vande Capelle - HIMA Paul Hildebrandt GmbH + Co KG, (2009)
- White paper, Functional Safety: Improve Industrial Process Plant Safety and Availability via Reliability Engineering, Dr. M.J.M Houtermans -

Risknowlogy, Mufeed Al-Ghumgham – Safco, T. Vande Capelle - HIMA Paul Hildebrandt GmbH + Co KG, (2008)

– White paper, Safety Availability versus Process Availability, introducing Spurious Trip LevelsTM, Dr. M.J.M Houtermans - Risknowlogy, (2006)
– SIL Manual, Safety Instrumented Systems, 3rd edition, GM International, technology for safety (2005)
– Kletz, Trevor A., Learning from Accidents, 3rd edition. Oxford U.K.: Gulf Professional. ISBN 978-0-7506-4883-7, (2001)
– Kletz, Trevor A., Lessons from disaster, How Organizations Have No Memory and Accidents Recur. Gulf Professional. ISBN 978-0884151548, (1993)