Practical experience with Deep Dive Assessments to identify key Major Accident Hazard risk factors on operational facilities

Graeme Laughland, Principal Process Safety Management Consultant, ABB Consulting, Belasis Hall Business Park, Billingham, TS23 4EB, UK

Keywords: Deep Dive, Safeguards, Assurance

Introduction

Process safety accidents continue at an unacceptable frequency in industry. Traditional methods for revalidation of Process Hazards Analysis/Process Hazards Reviews and auditing of Process Safety Management systems can involve considerable resources. In ever increasingly economically challenging circumstances businesses need to find new innovative best practice ways of ensuring a risk based approach is taken with Process Safety Management.

Sam Mannan (Director, Mary K. O'Connor Process Safety Centre) made this point as a keynote guest speaker at the IChemE's Hazards 25 conference. This paper will describe a 'Deep Dive Assessment' approach that has been developed to provide a rapid view on the 'vital signs' related to the state of health of measures to prevent and mitigate major accident hazards. The paper includes data from assessments conducted on major accident hazard processes and case study examples of findings. Conclusions are made with regards to what the Deep Dive approach reveals and the underlying safety management system root causes.

Background

Process safety accidents continue at an unacceptable frequency in industry (Marsh & McLennan Companies, 2016). Process safety incidents pose threats to all stakeholders of a business whether they be employees, management, contractors or shareholders. Significant incidents can often impact the local community either through harm to people and/or the local environment. Industry continues to struggle to prevent such incidents and as such it is reported that in certain countries that fines will increase further threatening businesses and their survival.

Repeatedly we hear senior management, public officials, regulators and members of community's state that such disasters "must not happen again!" However, in reality where a process facility exists industry endeavor's to control risks to a tolerably acceptable level. In doing so companies attempt to avoid major disasters from happening by conducting hazard identification and risk assessment processes and following industry good practice.

The high severity of major incidents often leads to more regulations and/or increased regulatory scrutiny which is an additional burden and cost for industry to bear so what can industry do differently? Learning from past disasters is often a topical theme at Process Safety conferences around the world and this sounds so simple but yet industry appears to struggle to deal with learning in a prompt and effective manner. Sam Mannan, (Director of the Mary Kay O'Connor Centre Process Safety Centre) said at his keynote speech at the IChemE's Hazards 25 conference that industry should seek new tools to assist with managing Process Safety. His call was for process safety professionals to be more innovative in their approach.

The incidents at Texas City in the USA and Buncefield in the UK in 2005 have been watershed moments for our industry. Following Buncefield, Gordon McDonald, chairman of the COMAH Competent Authority Strategic Management Group, Health and Safety Executive (HSE), UK, described what industry should focus on in a very succinct manner by putting forth three key questions for industry to answer:

1. Do we understand what could go wrong?
2. Do we know what our systems are to prevent this from happening?
3. Do we have information to assure us that they are working effectively?

Whilst addressing questions 1 and 2 is extremely important the topic of Deep Dive Assessments is primarily an assurance activity and as such aimed at addressing question 3.

Layers of Protection

Note that the nature of process safety incidents is distinctly different from occupational safety type incidents as illustrated in table 1 below which compares the characteristics of occupational safety and process safety incidents. With process safety incidents there are normally multiple failures which occur to result in a hazardous event. In other words there are issues with the many lines of defence which are often in place to protect us against such hazards. There are typically people failures at a number of levels of the organisation. Typically the front line staff will have made errors (immediate cause) and often over the longer term senior executives have made errors (systemic or root causes). These characteristics require a management approach that is better described as "risk management" than "safety management".

Table 1. Characteristics of Incidents

Occupational safety (e.g. slips, trips and falls)	**Process safety (e.g. major fire , toxic release, environmental spill)**
Low consequence, high frequency Low complexity Relatively frequent Often personal experience Victim as agent	High consequence, low frequency High complexity – multiple causes, active and latent failures Relatively rare Rarely personal experience Victim often not agent

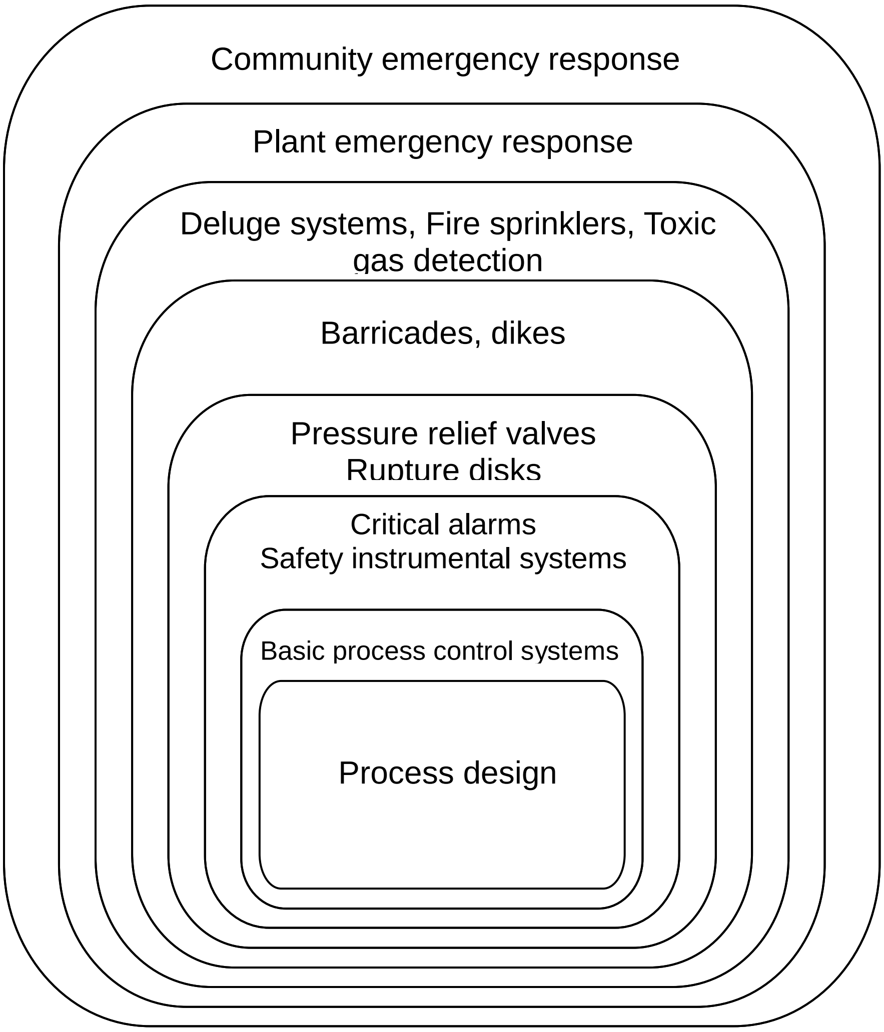
Professor Trevor Kletz wrote in the Loss Prevention Bulletin (Kletz, T., 2012) that "all higher mammals learn from experience including chemical engineers! Our desire must be to not learn from direct experience but to learn from others". So how can industry sharpen its focus on the key process safety risks that their assets present?

How can we help senior executives sleep more easily? Under the Control of Major Accident Hazard (COMAH) regulations in the UK industry has expended much resource with a strong focus on identifying hazards, assessing risks and ensuring that safeguards are put in place for their Major Accident Hazards. But how much effort has been expended on assuring ourselves that the safeguards work effectively? (I.e. the third key question, as presented by G.McDonald).

What tools could help us better understand how to effectively manage process safety? ABB Consulting have developed a new "Deep Dive Assessment" methodology to help address this question. It should be recognised that the complexities of Process Safety are such that a range of tools are required by Process Safety professionals. A Deep Dive Assessment may be viewed as being one part of a Swiss army knife or one tool in their tool box. A Deep Dive Assessment adds to the existing portfolio of tools available for use. No single tool provides a "magic wand" to address all process safety issues. Other existing tools include conducting routine Process Safety Management System Audits (CCPS, 2011), re-validating Process Hazards Analyses (Frank,W.L., Whittle D.K, 2001)/Process Hazards Reviews (Ellis, G., 2015) and using Process Safety Performance Indicators (Chemical Industries Association/HSE, 2006).The aim of a Deep Dive Assessment is to improve the control of a risk of a process safety incident by examining specific major accident scenarios and "drilling down" into the safeguards to make sure they are present and effective. The focus of a Deep Dive Assessment is on a company's key process safety risks. After all, if industry can't stay on top of its key risks where might that leave us?

The severe consequence and the complexity of causes of process safety incidents demand that multiple layers of protection are provided on top of the basic process design as illustrated in diagram 1. Safeguards such as safety instrumented systems (alarms, trips) and pressure relief devices may have low demands placed upon them such that their effective operation requires routine inspection and test. Failure of such layers of protection can be latent failures which may not be immediately apparent or revealed. Process operators may not have experienced certain upset conditions and therefore may not readily realise that an unplanned hazardous event is unfolding. The combination of layers of protection reduce the risk of a specific process safety incident and is often described as the "basis of safety".

Figure 1. Example Layers of Protection



COMAH safety reports will typically describe these layers of protection in depth and will have been originally identified through commonly used techniques such as HAZID, HAZOP, PHA and PHR. Table 2 shows practical examples of major accident scenarios and their associated layers of protection.

Table 2. Example Major Accident Scenarios and Layers of Protection

Safeguards	**Major accident scenarios and Layers of Protection**	
	Runaway reaction in Unit 04 leading to toxic release and multiple fatalities	Pool fire in Unit 12 distillation train leading to BLEVE in accumulator 12-T-07
Emergency response	Emergency Procedure 04.01	Emergency Procedure 12.15
Protective systems	-	Block 12D deluge system
Detection systems	Unit 04 toxic gas monitors 04-Q-1-12	Block 12D fire detection system
Secondary containment	-	Block 12D kerbing and emergency sump 12-D-04
Protective equipment	04-PSV-01	12-PSV-10
Equipment integrity	Reactor 04-R-01	Block 12 D piping system Accumulator 12-T-07
Safety instrumented systems	04-TAHH-01, 04-PAHH-01	-
Operating procedures	Operating Procedure 04-OP-01 and associated training	-
Process control system	04-TIC-01, 04-PIC-01, 04-FIC-01, 02.	-

Existing Assurance Activities

Under the COMAH regulations companies are required to have a Process Safety Management System. There are a variety of frameworks which companies could refer to in the development of their system and these have continued to evolve through time. Example Process Safety Management System frameworks include:

- OSHA Regulations, Standards - 29 CFR, Process safety management of highly hazardous chemicals. - 1910.119 (OSHA, 1992)
- Guidelines for Risk Based Process Safety , CCPS (CCPS, 2007)
- High Level Framework for Process Safety Management, Energy Institute (Energy Institute, 2010)

Process Safety Management System Audits

Traditional assurance or governance systems focus on auditing of the Process Safety Management System as a whole and not the control of specific risks. Significant audit time is spent on understanding how each element is managed and, by comparison, relatively little time is spent on detailed field verification of specific safeguards. So have the Process Safety Management Systems really been effective in protecting against the risk of specific scenarios?

Re-validation of PHAs

The concept of re-validating a PHA is described in literature (Frank, W.L., Whittle D.K, 2001). Within a PHA a HAZOP (IEC 61882:2016-03) study is one of the most commonly used techniques for identifying hazards and assessing risks. However the technique has many potential flaws, not least that every company has its own way of conducting HAZOPs. To illustrate this point we often find a variety of practices in place to record a safeguard. Take for example a pressure relief device of pressure safety valve (PSV) as they often known as. Table 3 shows a variety of ways in which this safeguard is recorded in a HAZOP. Given the large variation in practices of recording such a key safeguard from example 1 through to 5 shown in Table 3 then should it be a surprise to us that issues may arise in relation to the validity of the safeguard? One way to address this is for a company, or better still industry, to revise the standard for conducting HAZOPs. Have a common industry approach to documenting such information. It is incredibly ironic that HAZOPs can often recommend that a design meets with an industry standard but that the HAZOP technique itself does not follow a stringent industry standard with regards to how information is documented. Setting clear expectations for recording of this key information would be of great benefit to improving control of risks.

Table 3. Example HAZOP safeguard entries

Example Number	Example HAZOP safeguard entry	Comments
1	PSV	If no tag number exists, is getting routinely maintained. How could we locate design or maintenance records?
2	PSV 123456	Is the PSVs set pressure within the design limits of the equipment it is there to protect?
3	PSV 123456 with set point 30 barg	Sounds as if the HAZOP team have checked that the set point is acceptable?
4	PSV 123456 with set point 30 barg, sized for gas blow-through scenario	Sounds as if the HAZOP team have checked that the set point is acceptable and that the PSV is sized for the cause being discussed under the HAZOP entry.
5	PSV 123456 , set point 30 barg, sized for gas blow-through scenario, in SAP for routine maintenance	Sounds as if the HAZOP team have considered both design and maintenance aspects associated with the PSV.

Process Safety Performance Indicators

The topic of Process Safety Performance Indicators has been around for a number of years now and much focus has been given to this topic in the UK since the issue of guidance from the Chemical Industries Association and the Health and Safety Executive (Chemical Industries Association/HSE, 2006) in 2006. However, from discussions with many clients their struggle is in ensuring that they choose to focus on the right indicators. It would appear that industry is still going through a learning curve with regards to this topic.

Deep Dive Assessment Methodology

The methodology is very simple nature. Typically allocate 3 to 4 days to this activity. Plan the event with say 3 to 4 weeks' notice to help ensure that key individuals are involved. ABB Consulting typically utilises a Process Safety Management consultant and an Integrity Management consultant for the Deep Dive Assessment as they have a good blend of competencies to lead such assessments and provide an independent viewpoint. Select a small number of key risks for the facility. Typically anything from 3 to 10 scenarios. These are best selected from a COMAH safety report or some type of risk register for the facility.

Case study evidence from ABB's use of the Deep Dive Assessment methodology highlights that the more complex the event the more time is required for the Deep Dive. Events which have typically been subject to complex fault tree analysis, say involving reaction systems, for example, will require more time than events involving relatively simple storage tank operations. Judgements can be made as information is studied in preparation for a Deep Dive. In general look for the major "top 10" scenarios that have multiple fatality type and/or off-site impact type effects. Also look to include major accident scenarios that appear to have not been identified or are less well documented. Consider requests from the site in selecting scenarios for review and look for relatively complex scenarios with multiple layers of protection of different types. Try and select a mix of scenario type, for example a mix of fires, dust explosions and environmental spills. Try to ensure a selection and mix of scenarios that will involve multiple functions when examining safeguards e.g. Operations and Maintenance personnel, Technical staff (Process, Mechanical, Instrument, Control, Civil engineers, etc.) and members of the Management team.

The approach taken to selection of scenarios to assess can vary and can be influenced by the following factors:

1. Regulatory regime

Top Tier COMAH establishments within the UK will have a Safety Report containing a representative set of Major Accident Hazards. This section of the report provides quick and easy access to a summary of events to select from.

2. Company risk matrix

Companies who do not fall under the regulations requiring a Safety Case report but make use of their company risk matrix within PHAs or PHRs can plot their major hazard risks on a single matrix (refer to diagram 2) to help with the identification and selection of events.

Figure 2. Example Risk Matrix

	Catastrophic	5	L	M	H	H	H	H
	Critical	4	L	L	M	H	H	H
	Major	3	L	L	L	M	H	H
	Moderate	2	L	L	L	L	M	H
Severity	Minor	1	L	L	L	L	L	M
			F	E	D	C	B	A
	Frequency		$< 10^{-5}$ pa	$10^{-5} – <10^{-4}$ pa	$10^{-4} – <10^{-3}$ pa	$10^{-3} – <10^{-2}$ pa	$10^{-2} – <10^{-1}$ pa	10^{-1} or greater

3. Senior management and Process Safety professionals

The selection of events can be undertaken by senior management and Process Safety professionals to ensure that appropriate events are reviewed.

4. Previous incidents either within the company of within industry

Researching previous incidents inside and outside a company may help assist in identifying events that warrant assurance of controls at a site. Such searches may also reveal hazards that have not been identified or are less well understood.

Having gathered information on hazardous events to consider for Deep Dive Assessment it may be further necessary to select an appropriate number that fits with the timescale and resource available for the study. Experience has shown that there is no "one size fits all" approach to Deep Dive.

Safeguards for key risks will be recorded in documents such as COMAH reports or PHAs/PHRs. Simply take the safeguards claimed and scrutinise their validity. Note that such key risks can be relatively complex with numerous initiating causes. There may be fault trees constructed showing the various branches to the loss of containment scenario. Fault trees will help assessors quickly grasp the extent of the scenarios to evaluate. If initiating events are simply recorded in a HAZOP then more time may be required for preparatory activities to help identify all relevant safeguards.

In reviewing each claimed safeguard consider the design, operation and maintenance of each safeguard as follows:

- Question the design basis of each safeguard and hence the corresponding relevant good practice (code, standard, HSE guidance).
- Question the operational experience - is the safeguard known to be functional? How many demands have been placed on it? Are operators knowledgeable about how to respond if demands are placed on the safeguard? How would they know?
- Question the maintenance experience. Is the item being maintained? Are tests up to date? What do results reveal? Is there confidence about the safeguards reliability?

As issues are identified, and as time permits, attempt to drill down to understand the root cause of the issue. If time is not available to study the root cause of the issue in depth, then those involved in developing an action plan should consider this further and how they can best address any systemic issues that may have influenced the creation of the issue.

Case Studies

What do typical results look like despite the fact that other so called assurance activities get conducted? Table 4 shows some illustrative case study data in terms of numbers of recommendations made from Deep Dive Assessments.

Table 4. Case Study Data

Customer	Number of Sites	No of Drill Downs	Number of Recommendations	Comments
A	5	22	97	32 general, 65 specific
B	1	4	59	7 immediate risk
C	1	3	94	7 high priority
D	1	5	40	

Each Deep Dive is different as each company is in a different place with regards to their journey on PSM. These numbers highlight the benefit of using a different tool to review key major accident hazard risks and challenge if safeguards are adequate.

Case A

The company had revised their Process Safety Management System but wanted to know if they were in control of their key risks across 5 of their sites across the globe. Deep Dive Assessments highlighted on average 3 issues per drill down as well as some 32 general issues.

Case B

A top tier COMAH site in the UK. A company was concerned about findings from a regulatory inspection conducted by the HSE. They requested a Deep Dive of 1 site. Deep Dive Assessments uncovered 7 items which were categorised as an “immediate risk”.

Case C

A USA based bulk chemicals manufacturer who store and transport highly toxic chemicals. Deep Dive Assessments were conducted on 3 worst case scenarios and resulted in 94 recommendations. There were significant issues with applying the Layer of Protection Analysis (LOPA) technique and 24 recommendations were associated with this topic alone. Note that this facility had conducted 5 PHAs over the last 25 years. PHAs were re-validated every 5 years.

Case D

A lower tier COMAH site in the UK. Deep Dive Assessments revealed poor application of the Process Hazard Review technique such that significant risks were not clearly recognised.

Below are some example findings from Deep Dive Assessments. These findings show significant weaknesses through various barriers that had been claimed as a safeguard in a HAZOP study. In this case study bulk loading/unloading and storage tanks handling a highly toxic chemical were being reviewed. Modelling predicted a worst case potential impact on up to approximately 80,000 local residents.

Manual valves

The design basis for Car Sealed Closed (CSC)/Car Sealed Open (CSO) manual valves was not documented nor understood by operators and as such was out of compliance with the company’s standard. Random checking of some manual valves in the field showed that the field status was different compared to that shown on the P&IDs.

Alarms

Alarms had not been prioritised in accordance with industry good practice such as that defined in ISA18.2. Standard Operating Conditions (SOCs) had no description of the hazards nor was there an alarm response defined for the operators to follow.

Layer of Protection Analysis

Discussions revealed that for the recent LOPAs that had been conducted the actual demand rate differed from that claimed in the LOPA. Incorrect information had been used. A trip claimed in a LOPA study was not independent from the initiating cause and other Independent Protection Layers (IPLs). An alarm that was claimed as an IPL was not subject to routine test. Trip actions that were claimed were not valid. Incorrect information had been used. Fundamentally the LOPA technique was not being applied correctly.

Vessel inspections

Lack of appropriate vessel inspection/testing techniques. For the duty concerned the only concern for internal corrosion is Stress Corrosion Cracking (SCC), so the focus of internal inspections on floor welds should be for SCC, i.e., Wet Fluorescent Magnetic Particle examination. Perform phased array Non Destructive Examination (NDE) on the welds of the tank to test for SCC and welding quality during the scheduled external inspection as there is no documentation for the vessel.

Gas detection

There is no documented engineering basis for the siting of the toxic gas detectors. Conduct dispersion modelling to help ascertain the adequacy of the siting of existing detectors to help with early warning of a potential major release.

Emergency Procedures

Confirm what information is to be communicated in the event of a toxic emergency and with which external parties. Include this information in an emergency procedure. Provide training of personnel with regards to use of this information and conduct checks to ensure that personnel are familiar with what to do.

Wouldn't you be concerned if you managed a process and found as many recommendations as shown in table 4 associated with so few key risks? Upon completing the review of the safeguards for each hazardous scenario it is possible to re-plot the risk on a company risk matrix to help illustrate the relative importance of the findings. Prior to the Deep Dive Assessment the risk may have been viewed as being relatively low or in the green zone of the example risk matrix shown in diagram 3 below. The Deep Dive Assessment results however could in fact suggest that the actual risks associated with the facilities key risks are in fact high and in the red zone of a company's risk matrix.

Figure 3. Example Risk Matrix

Risk prior to Deep Dive Assessment

Actual risk - following Deep Dive Assessment

Severity	Catastrophic	5	L	M	H	H	H	H
	Critical	4	L	L	M	H	H	H
	Major	3	L	L	L	M	H	H
	Moderate	2	L	L	L	L	M	H
	Minor	1	L	L	L	L	L	M
			F	E	D	C	B	A
	Frequency		$< 10^{-5}$ pa	$10^{-5} - <10^{-4}$ pa	$10^{-4} - <10^{-3}$ pa	$10^{-3} - <10^{-2}$ pa	$10^{-2} - <10^{-1}$ pa	10^{-1} or greater

What advantages does Deep Dive Assessment bring? As it focuses on specific risks, Deep Dive Assessment complements other assurance activities such as PSM System Audits, the routine re-validation of PHAs and the use of PSPIs. It helps to maintain a very sharp focus on Major Accident Hazards and improves the understanding and documentation of them. It aligns with line management responsibilities for specific processes and assets and it directly exposes risks of Major Accident Hazards, thus providing real time assurance.

Examining multiple scenarios can also provide evidence of whether there are more systemic weaknesses as repeat type findings across similar types of safeguards may reveal this. Regardless of whether the Deep Dive Assessment discovers a systemic issue or not those involved in developing corrective action plans should be wary of providing a solution for a particular risk and should be encouraged to determine if wider systemic issues exist. Example systemic issues include:

- Lack of define competency criteria for LOPA leaders
- Ineffective training programs for operators on process specific hazards
- Inadequately defined responsibilities for process safety management system procedures

In summary, each Deep Dive Assessment can help facilities determine how well process risks are understood and documented and how well employees understand specific process risks. The assessment can identify if there are opportunities to further reduce specific process risks, to meet recognised good practice and to demonstrate that risks are as low as reasonably practicable. The assessment provides an insight into how well the assets are being managed and it can provide indications of weaknesses in management systems. A formal report follows each site visit with conclusions documented and supporting evidence provided. Reports contain a drill-down table for each specific scenario assessed.

Conclusions

In conclusion, Deep Dive Assessment complements existing Process Safety assurance activities. It helps to maintain a focus on Major Accident Hazards and improve the understanding and documentation of them. It aligns with line management responsibilities for specific processes and assets. It directly exposes risks of major accident hazards, thus providing real time assurance. The aim of this new methodology is to help industry sharpen its focus on its key risks and thus prevent major disasters. Results from case studies show that this flexible methodology has a proven benefit. The technique also highlights a root cause issue in that industry ought to standardise how safeguards are recorded within hazard identification and risk assessment techniques such as HAZOP. It is proposed that standardisation of this key issue would help improve the control of key major accident hazard risks.

References

1. Chemical Industries Association/HSE, 2006, Developing Process Safety Indicators, HSG254, 1st edition, ISBN 978 0 7176 6180 0.
2. CCPS, 2011, Guidelines for Auditing of Process Safety Management Systems, 2nd edition, ISBN 978-0-470-28235-9.
3. CCPS, 2007, Guidelines for Risk Based Process Safety, Wiley, ISBN 978-0-470-16569.
4. Energy Institute, 2010, High Level Framework for Process Safety Management, 1st Edition.
5. Ellis, G., 2015. Process SHE Guide 24, Leadership of Retrospective Hazard Reviews, ABB Consulting,
6. Frank, W.L., Whittle D.K, 2001, Re-validating Process Hazards Analysis, CCPS, ISBN 0-8169-0830-3.
7. IEC 61882:2016-03. Hazard and Operability Studies (HAZOP studies) - Application guide, 2nd Edition, ISBN 978-2-8322-3208-8.
8. Kletz, T., 2012, Improving Process Safety by Sharing Experience, Loss Prevention Bulletin Issue 227, IChemE.
9. Marsh & McLennan Companies, 2016, The 100 Largest Losses, 1974-2015, 24th Edition.
10. OSHA, 1992, US 29 CFR 1910.119 Process Safety Management of Highly Hazardous Chemicals.