Safety Science 77 (2015) 133–142

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

# A framework for safety automation of safety-critical systems operations

P.V. Srinivas Acharyulu [a,*], P. Seetharamaiah [b]

[a] Department of Computer Science and Engineering, GIT, GITAM University, Visakhapatnam, India
[b] Department of Computer Science & Systems Engineering, Andhra University, Visakhapatnam, India

ARTICLE INFO

*Article history:*
Received 8 July 2013
Received in revised form 2 February 2015
Accepted 20 March 2015

*Keywords:*
Safety-critical systems
Functional safety
Software safety
Software quality
Power plant operations

ABSTRACT

The more the risk level the lesser the safety and vice versa. The history of risk evaluation is moving from the point of accident investigation toward prior determination of quantum risk level. The risk level assessment is a part of risk evaluation process for identifying the risk aspects, impacts, hazard significance, and operational hazards. Risk assessment process helps for appropriate design of risk control procedures, to suggest provision of safety adequacy measures to reduce risk consequences, avoid or mitigate risks, and hazards. Risk free and failure free or fail-safe Operations in Safety-Critical Systems may not lead to loss of equipment, financial loss, environmental damage and hazard to human life. Prevailing standard techniques point out various risk factors and map out potential points where a safety critical operation can fail. The development of a framework is based on prevailing applicable standards and deals with safety–risk assessment for safety automation of safety-critical system operations. To explore various underlying risk factors, impacts and evaluation for determining risk magnitude, attributes and probabilities exhaustively considering practical conditions, a framework for safety automation of safety-critical operations is proposed. The methodology identifies underlying risk factors and determines risk significance for occupational and financial. Based on the identifications, a ten point scale to assess safety–risks is derived. The results of framework application to power plant case showed substantial improvement in assessing risks when compared to existing risk assessments. This is an indication of prevailing limited/inadequate safety–risk assessment in deeply addressing associated operational risks, proving the framework useful.



## 1. Introduction

A Safety Critical System is such a system which has the potential and may cause accidents either directly or indirectly. Failure of such systems can result in loss of life, property damage, environmental harm and financial loss. Safety is dependent on proper operations of such systems. Safety is always considered to the whole system including all safety critical operations. Some examples of Safety Critical Systems are *Defense* – Weapon Delivery Systems, Space Research Programs. *Production Industries* – Production, Manufacturing Controls, Maintenance and use of Robots. *Process Industries* – Power Generation, Chemical Process, etc. *Transportation* – Fly by wire Systems, Air traffic control systems, Interlocking systems, Automatic Railway Signaling Systems, Road traffic controls Systems, Vehicle Safety Systems. *Communications* – Ambulance Dispatch Systems, Online voice and data Communications. *Medicine* – Radiation therapy machines, Medical Radio Diagnostics, Medical Robots and so on. Some examples of automation technologies include (1) Automation Systems (2) Identification Systems (3) Human Controlled Systems (4) Industrial Controls (5) Industrial system Controls (6) Service Specific Requirement Systems (7) Sensor Systems (8) Power Control Systems (9) PC based automation, etc.

Automation of Safety Critical System operations needs a clear understanding when safety automation is considered. Automation of Safety involves computer hardware and software, electrical, electronic or mechanical equipment or devices. Hardware or Software if used to control safety critical system operations may contribute to hazard or cause other components to become hazardous. Hardware or Software deemed to be safe if hazard is quite impossible or highly unlikely. Safety automation involves embedded control systems. Safety automation relies on software for realization of safety to achieve their purpose with additional capabilities. A clear understanding of software development process is must to deliver quality software that can eliminate hazards by detecting potential hazard contributing software errors in safety critical systems operations effecting life, environment and property.

* Corresponding author.
*E-mail addresses:* pvschari@gmail.com (P.V. Srinivas Acharyulu), psrama@gmail.com (P. Seetharamaiah).

http://dx.doi.org/10.1016/j.ssci.2015.03.017
0925-7535/

Safety automation greatly depends on appropriate hazard analysis and risk assessment. Automation is transformation to smart, safe and sustainable emergence of profound changes for safety optimization. Automation technology utilizes safety controllers, programmable logic controllers (PLC), safety sensors, and design guarding systems to meet safety requirements. Risk assessment identifies potential hazards to reduce the risk and increase productivity. Automation addresses setup, operation and maintenance tasks combined with equipment or work environment and makes use of task based analysis by reviewing incidence reports. Moreover, identifies additional risks and assign risk ranking with the involvement of operational safety specialty expert. Facilitates in reporting scope of risk, overview of safety-critical operations and assign risk category and ensure evidence of probable risk.

Automating safety by application of computer controlled systems to assess risk levels so as to mitigate hazards is presented in this paper. Those operations if not operated in risk-free or fail-safe mode can lead to accidents or hazards. Examples of such safety-critical operations which may have negative effects on safety are considered for risk and safety level assessment. The parameters of such safety-critical operations including conditions in which they operate, intensity, impact & location, likelihood, consequence, detectability and significance are considered for review and detailed analysis is conducted. Consequently relative risk levels are assigned for each of the risk parameters. The results of the proposed framework indicated to be better than those of the prevailing limited scale weights and are shown in the results section. This framework can be applied to real-time systems with the factual measures and can assess the safety level and appropriate decision can be taken to apply computer controlled systems to handle such hazardous operations. Detailed vital risk contributing factors on a ten point scale of safety level is discussed which would give improved identifications of the overall safety critical system operation. Decisions can be taken to ensure adequate safety measures that can be applied at that point. This paper starts with general layout of safety critical system operations of power plant and attempts to identify risk for assessment and evaluation. It may be at the liberty of the organizations to adapt suitable safety automation techniques and technologies to suit their requirement to enhance safety by application of computers and software. Various identified risk aspects are shown in Table 1.

Safety Critical Systems Operation activities or functions in different conditions are shown in Table 2. It is identified that hazard consequences may occur in the conditions having intensity with low, medium and high degrees. Normal Operations are those which are being carried out as per planning, while abnormal activities which are beyond normal activities without directions of planning depending on the contingent requirements and above or below normal scheduled operations. Emergency activities are such actions which need to be taken on warranting situations whenever there is significant non-scheduled operation is observed. Direct nature is the involvement of employees working for the safety critical systems operations. Indirect employees including those working in the locations being employed by the contracting agencies, other public not connected with the operations, but connected to services of the equipment or personnel working for the operations. Routine nature of activities are those which are being carried out under normal working conditions as per schedules, though these normal works may involve hazards but inevitable. Non routine systems operations are those which shall be invoked under specific warranting situations and decisions for mandatory safety purpose or any other demonstrated cause.

**Table 1**
Risk aspects and coding.

| Serial no. | Description | Code |
|---|---|---|
| 1 | Air pollution | AP |
| 2 | Water pollution | WP |
| 3 | Work environment pollution | WEP |
| 4 | Land contamination | LC |
| 5 | Noise pollution | NP |
| 6 | Resource loss | RL |
| 7 | Legal | L |
| 8 | Fire hazard | FH |
| 9 | Occupational health & safety | OHS |
| 10 | Radiation | RD |

**Table 2**
Safety critical systems operations under various conditions.

| Nature/condition | | Meaning |
|---|---|---|
| N | Normal | Operations as per planning |
| A | Abnormal | Operations beyond routine and normal |
| E | Emergency | Warranting activities |
| D | Direct | Employees recruited |
| I | Indirect | Involvement of indirect employees |
| R | Routine | Regular and inevitable operations |
| NR | Non-routine | Specific operations under warranted decisions |

## 2. Terminology with respect to safety

*Failure*: An event where a system or subsystem component does not exhibit the expected external behavior and environmental conditions under which it must be exhibited should be documented in the requirements specification (Leveson and Turner, 1993). *Error*: An incorrect internal system state (Leveson and Turner, 1993). *Mishap*: Mishap is an unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property or damage to the environment (IEEE 100, 2000). *Hazard*: A system state that might, under certain environmental conditions, lead to a mishap (Leveson, 1986). Hence hazard is a potentially dangerous situation. *Risk*: Risk is the combination of the possibility of an abnormal event or failure, and the consequence(s) of that event or failure to a system's components, operators, users or environment (IEEE 100, 2000). *Safe*: Safe is having acceptable risk of the occurrence of a hazard (IEEE 100, 2000). *Safety*: Safety is the freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property (MIS-STD-882B, 1984). *Safety-critical*: Those software operations, that if not performed, performed out of sequence, or performed incorrectly could result in improper control functions (or lack of control functions required for proper system operation) that could directly or indirectly cause or allow hazardous condition to exist (Department of Defense, 1984). A real-time system is safety critical when its incorrect behavior can directly or indirectly lead to a state hazardous to human life (Software Safety, 1997). Decisions which shape the software architecture for safety-critical, real-time systems are driven in part by three qualities namely availability, reliability and robustness (Software Safety, 1997; Leveson, 1995). *Software Safety*: The application of the disciplines of system safety engineering techniques throughout the life cycle to ensure that the software takes positive measures to enhance system safety and that errors that could reduce system safety have been eliminated or controlled to an acceptable level of risk (Software Safety, 1997). *System Safety*: Application of engineering and management principles, criteria and techniques to optimize safety and reduce risks within the constraints of operational effectiveness, time and cost throughout all phases of the system life cycle (Software Safety, 1997)

The rest of the paper is organized as follows. Section 3 discusses on the available literature and review, Section 4 reviews background work, safety-critical systems operation of example power plant is described in Sections 5, proposed framework is presented

in Section 6, identified significant safety-critical operations are given in Section 7, comparison of risk level results are shown in Section 8, risk classification is determined in Section 9, discussion given in Section 10, and concluding comments are given in the end.

## 3. Materials and methods

National Aeronautics and Space Administration (NASA): **NASA-STD-8719.13A** (NASA, 1997) provides systematic approach to software safety as an important part of the overall system safety program. The NASA Guidebook, **NASA-GB-1740.13-96**, provides more details of applying this Standard (NASA, 1995). This standard is applicable to safety-critical computer systems. U.S. Department of Defense: **MIL-STD-882C** (Department of Defense, 1984) is primarily intended for System Safety, so a detailed software safety process is not addressed. However it provides a software hazard risk assessment process. It does not provide guidance or recommendations on the tasks and levels of analysis to perform for the determined software criticality. Detailed software safety process is not given. **DO-178B** – Development of Safety – Related Software in Airborne industries (Software Consider, 1992) provides guidelines for airborne systems. Good for software development and system safety assessment. No specific safety tasks are detailed. This standard is not applicable uniformly to all safety critical systems. Joint Software System Safety Committee (JSSC): **The JSSC Software System Safety Handbook** (Alberico et al., 1999). A Technical and Managerial team approach, providing management and engineering guidelines. No specific guidance is provided on determining the level of required software safety effort. **Motor Industry Software Reliability Association (MISRA):** MISRA compiles eight detailed reports containing information on specific issues relating to automotive software. It provides development guidelines for Vehicle Based Software (MISRA, 1994). It gives software life cycle but does not provide an explicit process for software safety that could be directly implemented. **APT Research, Inc.:** APT's 15 Step Process for Definition and Verification of Critical Safety Functions in Software was presented at the 2001 International System Safety Conference (Kuettner and Owen, 2001). The steps include identifying the system hazards, identifying software safety functional requirements, and tailoring the safety effort to criticality. The method shows the integration of the 15 step process for software system safety into the system safety process and the software life-cycle. International Electro-technical Commission (IEC) IEC61508 – Development of Safety-Related Systems on Ground **IEC 61508** (IEC, 1998) is intended to enable the development of programmable electronic safety related systems where application sector international standards may not exist, and to facilitate the development of application sector international standards. IEC 61508 defines requirements for the activities to be performed throughout the life-cycle in a similar way as DO178B does. In addition, for each life cycle phase it gives a set of techniques and measures that can be applied depending on the safety integrity level (SIL). The standards that are related to functional safety are shown in Fig. 1. DO-178 deal with aviation, **IEC 61511** with Process Industries, **IEC 60601** with medical, **IEC 50156** with Furnaces, **IEC 62061** with machinery, **IEC 60335** for house hold appliances, **IEC 61513** for nuclear power, and **IEC 50129** for railway systems. Automobile industries with **ISO WD 26262**

To overcome the limitations and to assess risks in a magnificent view points in minute hazard possibilities, we attempt to expand the risk assessment proportionate to functional circumstances that contribute to significance of risk assessment and evaluation. Significance determinants in any of the above standards which could contribute to hazards are not given in detail. We attempt to summarize functional parameters for each of the significance determinants, risk and safety assessments for the entire system safety of the critical operations under various conditions of demanding requirements. The proposed frameworks can be uniformly applied to any of the safety-critical systems operations especially for risk assessment and safety analysis. The development of the framework is based on prevailing applicable standards using an extended vision and by extending probabilities.

## 4. Background work

Certainly one of the most challenging tasks in safety science today is to develop ways of assessing systems in order to capture the patterns identified by social sciences following major accidents, to prevent them from causing disasters. In other words, the challenge is to develop ways to better grasp in foresight what is being interpreted in hindsight. This challenge is empirical, methodological, theoretical and epistemological (Le Coze, 2011, 2013). A safety assessment must rely on some form of indications about where to look and what to derive from observations. As a consequence, one has to specify key dimensions indicating relevant areas to be considered and investigated for safety assessment during empirical phases (Le Coze, 2011, 2013).

It is interesting to combine the generic models because, first, organizations need to implement certain feedback–feed forward functions in a coherent manner to ensure safety (this is the

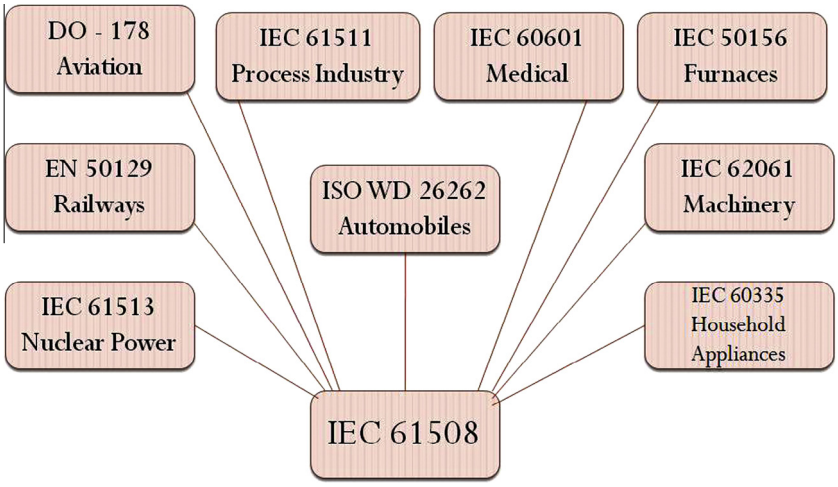


**Fig. 1.** Standards related IEC 61508.

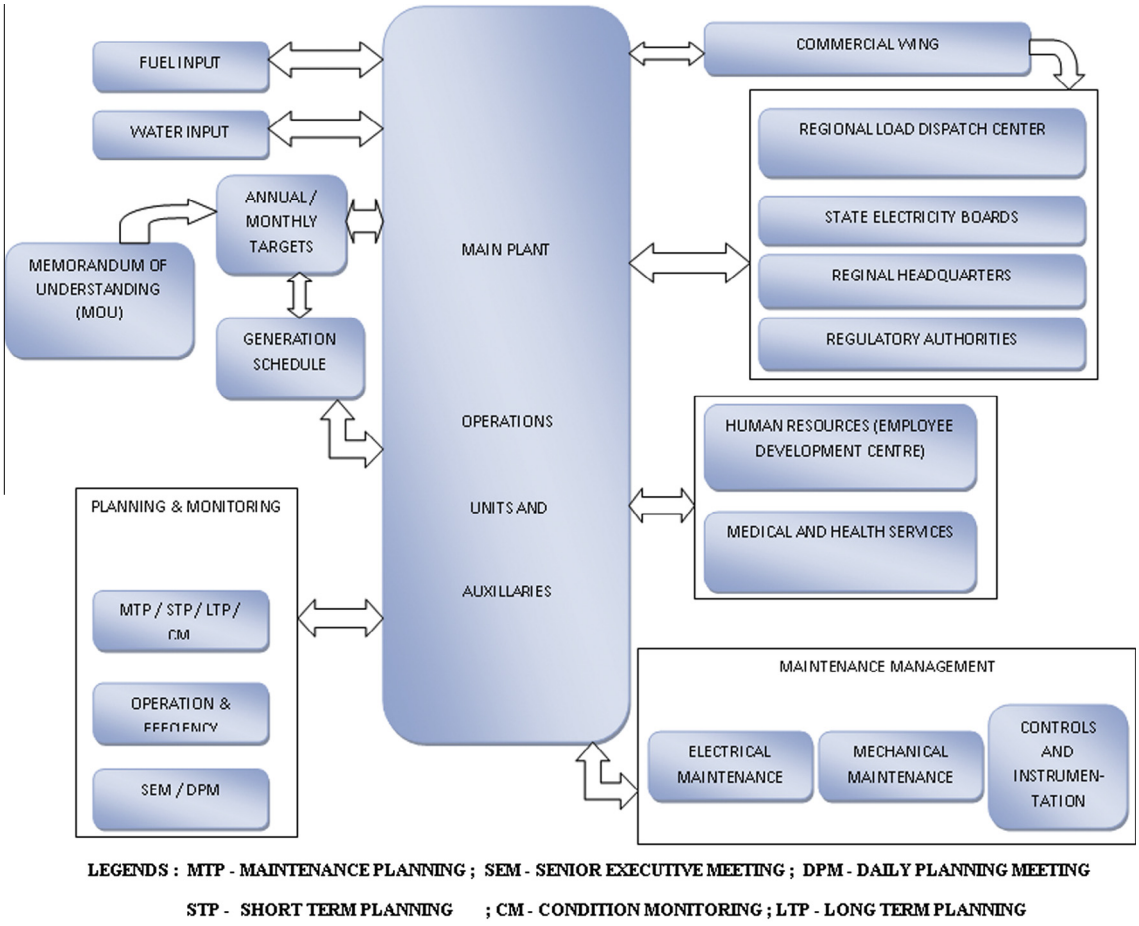


**Fig. 2.** Block diagram of power plant operations.

managerial view), and secondly, the implementation of these functions is the result of a particular technological design, tasks, and structural features of organizations, but also of cognitive, cultural and power issues at several nested layers of analysis (the sociological view). And, while Hale's model is indeed good at providing a normative point of view on safety through functions, it lacks the descriptive sociological content of Vaughan's model and its constructivist dimension (for an overview of constructivist discourses in industrial safety, see Le Coze, 2012, 2013).

In past years, the scope of these investigations has continued to expand, including organizations within their environment (Le Coze, 2008). This move can be seen in social scientists' contributions (Vaughan, 1996; Snook, 2000; Starbuck and Farjoun, 2005; Hopkins, 2008; Le Coze, 2010), but also in more normatively oriented models (Leveson, 2004). One notable outcome among sociological contributions to the study of disasters is Vaughan's attempt to outline the basics of a generic model of what is described as the 'dark side of organisations' (Vaughan, 1999; Le Coze, 2013).

Therefore for Hudson, safety culture can be engineered from top to bottom if supported by appropriate and specifically designed tools to motivate participation of employees. The outcome of this process is ranked at the level of a specific plant (or site) according to a scale from pathological (bad) to generative (good) safety culture. This 'culture ladder' associated with tangible criteria elaborated specifically for this purpose (Parker et al., 2006) enables organizations within the group to locate themselves to see how to improve or maintain their good safety culture. (Le Coze, 2013).

Rasmussen, who built on a multidisciplinary perspective to develop models of safety for assessment purposes, The core principles of his research were summarized in a key article in the field of safety science (Rasmussen, 1997; Le Coze, 2013).

some authors have now started to move in this direction and provide some guidance (e.g. Berman and Ackroyd, 2006; Dalzell and Hopkins, 2006; Reimann and Pia, 2007, 2009; Boin and Schulman, 2010), this research area still remains without a strong base. For instance, no systematic and analytical overview of models is available so far for this particular subject. Yet, this is a necessary step in clarifying different design rationales for safety assessment. (Le Coze, 2013)

Based on the analysis of articles produced over the past 10 years (Pidgeon, 1998; Reason, 1998; Cox and Flin, 1998; Gherardi et al., 1998; Hale, 2000; Guldenmund, 2000; Glendon and Stanton, 2000; Richter and Koch, 2004; Hopkins, 2006; Hudson, 2007; Haukelid, 2008; Antonsen, 2009), and without excessive simplification, a basic layered model of interactions between 'attitudes', 'beliefs', 'norms' and 'values' of Safety Culture can be put forth here as a widely shared basic theoretical outcome of Safety Culture. (Le Coze, 2013)

## 5. Operations in safety critical systems

As an example case to validate the framework, the general layout of power safety-critical systems operations of Ramagundam Super Thermal Power Station (RSTPS) unit of NTPC Limited

http://www.ntpc.co.in is shown in Fig. 2 including those divisions involve in its operations. There are as many as nineteen divisions involved in operation external to the power generating plant, its units and auxiliaries. Each of these divisions monitors for generation failure risks with their independent functioning making an impact on smooth functioning of the overall safety critical functioning of the entire power plant. All of these nineteen divisions are directly or indirectly involved in various operations of the main power plant. The main power plant has again as many as twenty five divisions rendering their best services for the smooth functioning of the entire power plant. These safety critical systems operations required to assess the risks, their impacts and evaluating them to eliminate while identifying their significance. These risk aspects are shown in Table 1.

### 5.1. External functionalities to operations

The regulatory authorities, statutory bodies, commercial viability, regional controls, dispatch load center, state electricity boards, memorandum of understanding which fixes the daily, monthly and annual target power generation leading to generation schedule constraints. Moreover, planning and monitoring makes further constraint on scheduled overhauling, maintenance planning, operation & efficiency, senior executive meeting decisions, and daily planning meetings, permit to works and work order card schedules. Maintenance management consisting of electrical & mechanical maintenance and controls & instrumentation wing raises overriding controls over the planning with the approvals in daily planning meetings and senior executive meetings. The most critical part of power generation greatly depend on fuel management and water input which are vital resource components of power generation and thus has direct impact on the generation, resource or revenue losses and forms financial constraints in addition to the functional risks.

### 5.2. Internal functionalities to operations

Combustion Fuel management involve in fuel handling systems operation and their maintenance activities. These activities are safety critical such as fuel transportation, fuel resource storage, maintenance of systems which may lead to revenue loss, occupational health and safety issues while in operations if not operated risk-free or fail-safe. As the input is natural water, need to be purified before converting into steam to avoid corrosion of power generating equipment. The purification process involves chemistry are chemical analysis of the fuel quality, natural water, de-mineralization, boiler chemistry and steam water chemistry. These activities may contribute to risks and hazards associated with occupation, environmental pollutions, equipment and to people in and around the operations. Planning and Monitoring plays a very important role in co-ordination for the efficient power plant management for Long Term Planning (LTP), Short Term Planning (STP), Spare/Inventory Review/Monitoring (SMG), Streamlined Reliability Centered Maintenance (SRCM), Risk Evaluation and Prioritization (REAP), Condition Monitoring (CM) and Financial Risk Optimization (FRO). These activities are safety-critical in one way or the other, may cause risk to environment, health & safety, equipment robustness, and proper budget utilization if operations are not planned or fail in proper risk assessment. Maintenance involves electrical, mechanical, civil, controls and instrumentation engineering areas, contributes to maintain equipment robustness for safe operations. Safety of people and environment becomes prey for risks if these maintenance works are not carried out in a systematically planned way. The decisions may go wrong if stringent actions as per planning & monitoring schedules are not carried out, may lead to accidents.

### 5.3. Mixed functionalities to operations

Human Resource & Employee Development Center (HR & EDC) activities include utilization of allocated budget for Corporate Social Responsibility (CSR) for conducting welfare awareness activity in the surrounding villages, conducting medical camps, proportionate tree plantation, to develop and maintain bipartite culture in the organization, to inculcate a sense of involvement and effective participation Since this is purely administrative in nature and as such no safety issues are involved except to impart training and conducting campaign to cope up with the safety requirements and conducting safety awareness programs in and around. The medical and health services conduct mandatory health examination to all employees, contracting agencies such as canteen and employed security personnel, to conduct family welfare camps, and to segregate biomedical waste to avoid pollution which is good medium for subjecting occupational health risks. Medical robots can be applied for removing these biomedical wastes. Reporting of hazards associated with occupational safety of the working employees and other agencies shall work as feedback for upgrading or renovate the existing procedures to improve safety.

Memorandum of Understanding (MOU) is arrived at before the establishment of the power plant and fixes the target generation monthly and annually depending on the power requirement by the state, central governments and public for their needs. These pre-assigned target achievements are stringent and influence pressure on the operations of the power plant. Thus daily, monthly and annual minimal power generation has to be ensured, though the supply of fuel has constraint for balancing between supply and demand, scarcity of water, further more constraint on balancing the input water requirement and storage. The MOU fixes the target generation and the rest of achieving the targets is at the responsibility of the management. Commercial wing directly involve in the operation and maintenance activities as well in administrative area for the feasibility study & analysis of the day to day generation activities and interfaces with the Regional Load Dispatch Centre (RLDC), State Electricity Boards (SEB), Regional Head Quarters (RHQ) and with Regulatory Authorities such as Central Electricity Authority (CEA). In turn these four independent bodies interface with the direct operations and maintenance activities of power plant, monitor continuously and constantly. Risks associated are mostly legal and administrative.

The main function is to generate the power as per the agreed targets in MOU in Million Units (MU), to maintain the target heat rate, Specific Oil Consumption and De-mineralized (DM) Water consumption with zero accidents in Operation activities. The prime responsible activities are (1) Safe and Efficient Operation of the Units (2) Effective re-commissioning after Overhauling (OH) (3) Effective start-up and shutdown as per the guidelines (4) Organizing safety talks for awareness (5) Ensure usage of Personal Protective Equipments (PPEs) (6) Compliance with Permit to Work System (PTW). The associated risks include all those specified in Table 1 if the safety critical operations are not carried out in co-ordination and compliance with the planning, derived requirements, statutory guidelines and in accordance with the law and standards.

## 6. Proposed framework

During the entire process of proposed framework, the prevailing practices and assessment procedures are taken into consideration. The proposed framework is based on the findings of hazards analysis by defining the factors for identification of significance, location wise accidents implication whether hazardous or non-hazardous, likelihood of accident or failure, hazard detectability

and consequences while classifying them. The proposed framework facilitates in assessing the risk level for any safety critical system operation. The proposed framework is an extension of the mentioned parameters in three degrees of impact intensity with relevant assumed risk levels. First the framework attempt to identify the significant aspects impacts analysis and are tabulated accordingly. The tasks to be carried out are

(1) Identification of hazard significance.
(2) Identification of risk location.
(3) Identification of risk likelihood.
(4) Identification of risk detectability.
(5) Identification of risk consequence.
(6) Risk classification.

### 6.1. Identification of Hazard Significance

*Hazard Significance* depends on five parameters namely extent, intensity/effect, frequency or number of occurrences per year, duration of hazard and resource or revenue loss with the three degrees of impacts intensity. Consequently corresponding risk level/weight is assigned. The details are shown in Table 3.

Resource/Revenue Loss (RL) are in terms of monetary loss and depend on the viability of the project. Significance is calculated as the product of these four parameters.

$$\text{Significance} = E * I * F * D$$

Any value other than zero for the product EIFD is regarded as unsafe and need to be declared as significant. Other parameters such as Resource Loss (RL) and Legal (L) cannot be predicted in advance and hence these too are noted as Significant. All other minor activities which does not involve in any of the E, I, F, D, RL and L are treated as Non-Significant (NS) though they are safety-critical. The parameters specified above may vary from situation to situation and corporate to corporate, definitely depend on the decisions of the competent authorities concerned and responsible for carrying out the set out objectives. While designing software for safety critical systems, the prime need is to identify the significance of each of the operations and their effects. The above significance determinants are most useful for safety automation applications.

### 6.2. Identification of risk location

Accident/hazard occurrence location plays very important in determining the risk assessment, whether it may hazardous (H) or non-hazardous (NH). These locations are identified and assigned relevant risk weight. If the accident occurs on the spot, attributes to NH the risk level is higher and highest if it is hazardous. If the aspects impact occurs outside the factory, non-hazardous the risk level is lowest while if hazardous the risk level is moderately higher. Table 4 shows various location wise accident risk weights.

While application of safety automation the effects of the accident at locations which has effects in different extents are contributing to the significance of the risk whether hazardous or non-hazardous.

**Table 3**
Hazard significance indicator.

| Code | Meaning/units | Risk level weight (Wt) | | |
|---|---|---|---|---|
| | | Measurement | Intensity | Wt |
| E | Extent/area | <0.5 km | Low | 1 |
| | | ⩾0.5 km & <3 km | Medium | 2 |
| | | ⩾3 km | High | 3 |
| I | Intensity/effect | Temporary | Low | 1 |
| | | Permanent | Medium | 2 |
| | | Fatal | High | 3 |
| F | Frequency/no. of occurrences per year | <5 | Low | 1 |
| | | ⩾5 & <15 | Medium | 2 |
| | | ⩾15 | High | 3 |
| D | Duration/time | <5 min | Low | 1 |
| | | ⩾5–60 min | Medium | 2 |
| | | ⩾60 min | High | 3 |
| RL | Resource/revenue loss | <100,000 | Low | 1 |
| | | ⩾100,000 | Medium | 2 |
| | | ⩾5,000,000 | High | 3 |

**Table 4**
Accident location risk level.

| Location code (Scale) | Accident location & consequence | Implication/ risk level | |
|---|---|---|---|
| | | NH | H |
| S1 | Spot | 4 | 8 |
| S2 | Within department | 3 | 7 |
| S3 | Within factory | 2 | 6 |
| S4 | Outside factory | 1 | 5 |

### 6.3. Identification of risk likelihood

Hazard occurrence likelihood is identified as four categories such as highly unlikely, unlikely, likely and very likely depending on the systems conditions applicable to that particular situation or operation. These may have aspects impact intensity which may be low, medium or high contextual to the nature of operations, location and its significance with relevant risk weight assigned. Table 5 depicts these which are extended in Table 9 for assessing overall risk. As such there is no risk levels assigned for the degrees of impact intensity.

Determination of likelihood of failure occurrence with various intensities contribute to significance and thus helpful in risk assessment for any safety critical applications.

### 6.4. Hazard detectability identification

If Hazard occurrence is detectable and easily be avoided or necessary action can be taken to control. Otherwise the aspects impact may not be predictable and thus has highest risk level. Table 6 describes detectability risk levels. Hazard detectability is extended in the Table 11.

### 6.5. Identification of consequences

Consequences of hazard may have the range from discomfort to fatal with low, medium and high for aspects impact intensity and

**Table 5**
Risk likelihood ranking.

| Code & meaning | | Impact intensity | Risk level |
|---|---|---|---|
| HUL | Highly unlikely | Low<br>Medium<br>High | 1 |
| UL | Unlikely | Low<br>Medium<br>High | 2 |
| L | Likely | Low<br>Medium<br>High | 3 |
| VL | Very likely | Low<br>Medium<br>High | 4 |

**Table 6**
Risk detectability ranking.

| Detectability code/meaning | | Risk level |
|---|---|---|
| D1 | Immediately | 1 |
| D2 | Highly | 2 |
| D3 | Low | 3 |
| D4 | No detectable | 4 |

**Table 7**
Risk consequence ranking.

| Consequence level | | Impact intensity | Risk level |
|---|---|---|---|
| C1 | Discomfort | Low<br>Medium<br>High | 1 |
| C2 | Minor injury | Low<br>Medium<br>High | 2 |
| C3 | Reportable | Low<br>Medium<br>High | 3 |
| C4 | Major injury | Low<br>Medium<br>High | 4 |
| C5 | Permanent disability | Low<br>Medium<br>High | 5 |
| C6 | Fatal | Low<br>Medium<br>High | 6 |

corresponding relevant risk level weight is assigned and shown in Table 7. These consequences or exposure to consequences are further extended in Table 10.

Total Risk Level is calculated as per the following formula. The lower the risk level, the higher the safety of the operations. The higher the risk level, safety is of more concern.

$$\text{Total Safety Level} = \text{Weight of the Location} + \text{Severity} + \text{Weight of Detectability}$$
$$(\text{Severity} = \text{Likelihood} * \text{Consequence})$$

Risk and safety assessment can be calculated on the assigned values as per the formula for each of the safety-critical operations. Ranges for safety and non-safety can be derived. The assigned weights are not to scale or the actual weights. The entire procedure is for a demonstrative and comparative analysis with extended situations and predictions according to practical situations and conditions.

### 6.6. Risk classification

Risks are identified as four categories as trivial, moderate, substantial and potential as shown in Table 8 with their intensities and relevant risk level weights assigned. If the consequence is trivial and impact intensity is low the risk level is low. If the consequence is potential and impact intensity is high the risk level is very high. It is not essential that one activity need not contribute to only one or to all identified impacts and thus relevant activities corresponding to impacts are considered.

### 6.7. Decomposition of likelihood

Only four levels of failure likelihood are inadequate in addressing the risks. These levels are extended basing on the appropriate probability of failure likelihood and risk levels are ranked accordingly. Likelihood of failure prediction has crucial role in determining the severity and significance which contribute greatly to safety assessment.

**Table 8**
Risk classification ranking.

| Risk classification | | Intensity | Risk level |
|---|---|---|---|
| T | Trivial | Low | 1 |
| | | Medium | 2 |
| | | High | 3 |
| M | Moderate | Low | 4 |
| | | Medium | 5 |
| | | High | 6 |
| S | Substantial | Low | 7 |
| | | Medium | 8 |
| | | High | 9 |
| P | Potential | Low | 10 |
| | | Medium | 11 |
| | | High | 12 |

**Table 9**
Decomposition of likelihood probability.

| Identified likelihood | | Decomposition of likelihood probability | | |
|---|---|---|---|---|
| Code | Risk level | Extended code | Meaning | Risk level |
| VL (Very likely) | 4 | DL | Definitely Likely | 10 |
| | | VHL | Very highly likely | 9 |
| | | HL | Highly likely | 8 |
| L (Likely) | 3 | MHL | Moderately high | 7 |
| | | MML | Moderately low | 6 |
| UL (Unlikely) | 2 | LL | Likely low | 5 |
| | | VLL | Very low likely | 4 |
| HUL (Highly unlikely) | 1 | RCL | Remote chance of likely | 3 |
| | | VRCL | Very remote likely | 2 |
| | | ANL | Very highly un-likely | 1 |

### 6.8. Decomposition of consequences

Hazard Consequences are identified after rigorous study as six levels without differentiation of the three degrees of impact. Further, consequences are extended depending on various situational effects without consideration of the degrees of impact is shown in Table 10. Decomposition mainly based on the deeper practically sustained injuries or hazards. Definitely the extension would contribute to enhance safety for application of automation activities of operations.

**Table 10**
Decomposition of hazard consequences.

| Identified consequences | | Decomposition of consequences | | |
|---|---|---|---|---|
| Code | Risk level | Hazard code | Consequences | Risk level |
| C6 | 6 | HS | Hazard sudden | 10 |
| | | HW | Hazard with warning | 9 |
| C5 | 5 | VH | Very high | 8 |
| | | HH | High hazard | 7 |
| C4 | 4 | MH | Moderately high | 6 |
| | | LH | Low hazard | 5 |
| C3 | 3 | VLH | Very low | 4 |
| | | MH | Minor hazard | 3 |
| C2 | 1 | VMH | Very minor hazard | 2 |
| C1 | 0 | NH | No hazard | 1 |

**Table 11**
Decomposition of detectability.

| Identified detectability | | Proposed detectability | | |
|---|---|---|---|---|
| Code | Risk level | Extended detectability | Meaning | Risk level |
| D4 | 4 | HI | Highly impossible | 10 |
| | | VR | Very remote | 9 |
| | | R | Remote | 8 |
| D3 | 3 | VL | Very low | 7 |
| | | L | Low | 6 |
| D2 | 2 | M | Moderate | 5 |
| | | MH | Moderately high | 4 |
| D1 | 1 | H | High | 3 |
| | | VH | Very high | 2 |
| | | AD | Almost detectible | 1 |

### 6.9. Decomposition of detectability

Detectability can be decomposed into finer elements of possibilities as shown in Table 11. Initial detectability levels are designated as four levels and each of these levels are decomposed into ten levels with an inner view of the possibility. Their relative rankings are assigned. Determination of significance greatly depends on the detectability of a failure. When failure or associated risk is detectible the probability of risk can be avoided or mitigated or the operation can be aborted. When safety automation concerns detectability on microscopic examination of the possibilities of failure, if ranked accordingly can suggest a suitable applicability of safety measures.

## 7. Identification of significant safety critical systems operations

Some of the safety-critical activities or product or a service identified in the example power plant are shown in Table 12. Safety automation applicability can be derived from the significant activities and based on the risk ranking or level. Impacts of these activities and their implication also shown with relevant risk level weights calculated as EIFD. Significance of the activity and its priority need to be decided basing on the effect, consequence, aspects and classification. In broad the lesser risk/significance level as 1 in case of explosion is of least significance, but the effect itself is significant as it involves more than one contributing factor. The higher the value of EIFD the higher the significance as its consequence is in all dimensions such as extent, intensity, frequency and duration. For one activity such as combustion in boiler has the effects legally, air pollution, occupational hazards and also loss of equipment, revenue and resource in addition to loss of life. Thus in conclusion such activities though contribute to lowest risk level, is significant. The results of proposed framework clearly indicated with increased risk level in Table 13.

In the above Table 12 emissions due to combustion involves risks in legal impacts, air pollution, work environment pollution, area effected, intensity, frequency and duration of the incident makes the activities significant. Relative significance level is assigned to concentrate and prioritize the activity for safety automation purpose.

Table 12 shows the example safety critical activities. It may be observed that some of the safety-critical activities may have one or more of impacts. Condition or nature in which they operate also takes part with consequences related to that particular activity. Risks associated with specific activity are identified with their consequences. Significance of risk is shown with three degrees of impacts. Only significant operations are shown for identified activities or services or operations.

**Table 13**
Calculation of risk level for the example activity.

| Activity/product/service and hazard | Impact | S | As per existing | | | | As per proposed framework | | | | Risk Level |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | L | C | D | Risk | L | C | D | Risk | |
| Combustion in boiler | Legal | | – | – | – | – | – | – | – | – | – |
| Flue gas emission from the stack | | | | | | | | | | | |
| | AP | | 2 | 4 | 3 | 2 16 | 9 | 5 | 5 | 52 | 36 |
| Hot air leakage | WEP | | 1 | 1 | 2 | 2 5 | 2 | 3 | 5 | 12 | 7 |
| Ash slurry pump house | WP | | 5 | 3 | 6 | 3 26 | 7 | 9 | 7 | 75 | 49 |
| Overflow of fly ash slurry | | | | | | | | | | | |
| Slurry pump overflow | LC | | 5 | 3 | 5 | 4 24 | 6 | 8 | 9 | 62 | 38 |
| Air conditioning plant operation | NP | | 4 | 4 | 6 | 1 30 | 9 | 9 | 1 | 86 | 56 |
| Sound from AC compressors | | | | | | | | | | | |
| Combustion in boiler | RL | | – | – | – | – – | – | – | – | – | – |
| Excess coal consumption | | | | | | | | | | | |
| Oil firing | FH | | 6 | 4 | 6 | 2 32 | 9 | 9 | 5 | 92 | 60 |
| Leakage of oil from the guns | | | | | | | | | | | |
| Explosion (fatal, property damage) | OHS | | 8 | 4 | 6 | 4 36 | 9 | 9 | 9 | 98 | 62 |

Legend: L – Likelihood; C – Consequence; D – Detectability S – Scale.

## 8. Comparison of risk levels with existing and proposed framework

Table 13 shows calculated results for risk levels as per the existing findings and proposed framework. It is observed that substantial increase in the risk assessment for safety critical systems operations and helpful in applying automation techniques/technologies. It is proved that the proposed framework is better in supporting risk assessment for safety critical operations by identifying significant activities in advance so as to adapt suitable safety adequacy measure.

## 9. Risk classification according to proposed framework

Risk classification is shown in Table 14 along with consequence, impact and applicable safety adequacy measure for the identified

**Table 12**
Significance indicator for the example safety critical activities.

| S. no | Activity/product/service | Aspect/effect | Impact | RL | E | I | F | D | Level = EIFD | S/NS |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Combustion in boiler | Flue gas emission from the stack | L | – | – | – | – | – | – | S |
| | | | AP | – | 2 | 3 | 3 | 3 | 54 | S |
| | | Hot air leakage | WEP | – | 1 | 3 | 3 | 3 | 27 | S |
| 2 | Ash slurry pump house | Overflow of fly ash slurry | WP | – | 1 | 1 | 2 | 2 | 4 | S |
| 3 | Ash slurry pump house | Slurry sump overflow | LC | – | 2 | 2 | 3 | 3 | 36 | S |
| 4 | Air conditioning plant operations | Sound from AC compressors | NP | – | 2 | 2 | 3 | 3 | 36 | S |
| 5 | Combustion in boiler | Excess coal consumption | RL | Cost | – | – | – | – | – | S |
| 6 | Oil firing | Leakage of oil from the guns | FH | Cost | 1 | 3 | 2 | 3 | 18 | S |
| 7 | Combustion in boiler | Explosion (fatal, property damage) | OHS | Cost | 1 | 1 | 1 | 1 | 1 | S |

RL – Resource loss; E – Extent; I – Intensity; F – Frequency; D – Duration; S – Significant; NS– Non-significant.

**Table 14**
Comparison of safety levels with hazard consequences, impacts and safety adequacy measures.

| S. no. | Activity/product/service | Hazard consequence | Impact | Risk degree/safety measure | |
|---|---|---|---|---|---|
| | | | | Classification | Applicable safety adequacy |
| 1 | Combustion in Boiler – flue gas emission from the Stack | Unknown/suffocation (C1) | L, AP | Trivial | Personal protective equipment/application air pollution detection systems sensors |
| 2 | Combustion in boiler – hot air leakage | Burn injuries (C2) | WEP, RL | Moderate | Personal protective equipments, austerity measures |
| 3 | Ash slurry pump house | Water pollution (C3) | WP | Substantial | Pollution detection systems |
| 4 | Ash slurry pump house | Land contamination (C3) | LC | Substantial | – |
| 5 | Combustion in boiler | Hearing loss (C5) | NP | Potential | Personal protective equipments |
| 6 | Oil firing | Resource loss (C3) | RL | Substantial | – |
| 7 | Combustion in boiler | Burn injuries, property damage, fire & explosion (C3,C4,C5,C6) | FH | Potential | Scope for safety automation measures/alternate safety devices/alarms, etc. |

significant safety critical systems operations. In case of air & water pollution, computer controlled pollution detection systems are applicable while for fire hazards computer controlled smoke detection systems, safety alarms and alternate safety devices such as fire fighting systems can be applied. For other consequences personal protective equipments are applicable to ensure safety.

## 10. Discussion

The results of proposed framework to those of existing risk levels indicated the increase in risk level of the activity, and thus warrant in safety automation wherever applicable for the use of computer controlled systems to minimize accidents and to improve safety or reduce risk levels. Table 14 indicates detailed applicability of safety measure wherever possible with the details of activity, consequence of the hazard if happens, impact, risk classification and safety adequacy measure available and applicable. Safety Adequacy measures can be provided alternatively for the hazards which are unavoidable except to provide protective equipments. The Table 12 describes the safety aspects impacts analysis whether hazardous/non-hazardous and significant/non-significant depending upon the intensity of the impact. Significance need to be decided by authority competent to assign the value. Table 12 covers each of the impacts of risk on environment, human life, financial loss or equipment damage. Safety levels are calculated based on the prevailing safety analysis with their relative weights and as per the framework is shown.

## 11. Conclusion

The framework provides clarity to improve safety of human, environment, equipment, identified aspects and regulatory compliance. The framework facilitate to give documented evidence of safe operations for routine jobs and updates risk assessment when operational changes which reflect new risks and identifies potential risks that could have been missed by other methodologies. The framework provides information to identify significant operations, risks, risk ranking, aspects impact, risk classification and suggesting safety adequacy measure. The framework facilitated to review existing risk category and compare with that of deeply addressed risk probability basing on likelihood, consequence and detectability. The framework report attracts attention of safety measures to be taken up for each of the safety critical operations.

Safety automation for safety critical systems operations require very high expertise, in addition to technical know-how, methodological and strong logical extensions to provide improved safety to satisfactorily acceptable levels. This paper contributes to extend the various risk contributing factors, which provide micro examination of effects whether low, medium or high intensity of hazards. Since the significance is identified in advance, this paper contributes to pin point and prioritize the safety activities in that area. This paper facilitates for further extending the risk weights for degree of impacts. A similar approach can be adapted for other safety critical systems. This work can be further extended to address implementation costs and time. Rigorous work is needed to meet the complete set of safety automation requirements leading to standardization of the framework.

## References


Alberico, D., Bozarth, J., Brown, M. et al., 1999. JSSC Software System Safety Handbook. A Technical and Managerial Team Approach (December).

Antonsen, S., 2009. The relationship between culture and safety on offshore supply vessels. Saf. Sci. 47 (8), 1118–1128.

Berman, J., Ackroyd, P., 2006. Organisational Drift – A Challenge for Enduring Safety Performance. IChemE Symposium Series No. 151.

Boin, R.A., Schulman, Paul., 2010. Assessing NASA's safety culture: the limits and possibilities of high reliability theory. Public Administration Review 68 (6), 1050–1062.

Cox, S., Flin, R., 1998. Safety culture: Philosopher's stone or man of straw? Work and Stress 12 (3), 189–201.

Dalzell, G., Hopkins, A., 2006. Is Hazard Management Working? IChemE Symposium, Series No. 151.

Department of Defense, 1984. System Safety Program Requirements MIL-STD-882C.

Department of Defense, 1984. "System Safety Program Requirements" MIL-STD-882C.

Gherardi, S., Nicolini, D., Odella, F., 1998. What do you mean by safety? Conflicting perspectives on accident causation and safety management in a construction firm. Journal of Contingencies and Crisis Management 6, 202–213.

Glendon, A.I., Stanton, N.A., 2000. Perspectives on safety culture. Saf. Sci. 34, 193–214.

Guldenmund, F.W., 2000. The nature of safety culture: a review of theory and research. Saf. Sci. 34, 215–257.

Hale, A.R., 2000. Culture's confusion. Saf. Sci. 34, 1–14.

Haukelid, 2008. Theories of (safety) culture revisited—an anthropological approach. Saf. Sci. 46 (3), 413–426.

Hopkins, A., 2006. Studying organisational cultures and their effects on safety. Saf. Sci. 44, 875–889.

Hopkins, A., 2008. Failure to Learn. CCH.

Hudson, P., 2007. Implementing a safety culture in a major multi-national. Saf. Sci. 45, 697–722.

IEC, 1998. International Standard, Functional Safety of Electrical/Electronic/Programmable Electronic Safety – Related Systems – IEC 61508-3; Part 3 Software Requirements.

IEEE 100, 2000. "The Authoritative Dictionary of Standard Terms". IEEE Press.

Kuettner Jr. H.D., Owen, P.R., 2001. "Definition and Verification of Critical Safety Functions in Software". In: Proceedings of the International System Safety Conference (ISSC) 2001. System Saf. Sci., Unionville, Virginia, pp. 337–346.

Le Coze, J.C., 2008. Organisations and disasters: from lessons learnt to theorising. Saf. Sci. 46, 132–149.

Le Coze, J.C., 2010. Accident in a French dynamite factory: an example of organisational investigation. Saf. Sci. 48 (2010), 80–90.

Le Coze, J.C., 2011. A study on the impact of changes on industrial safety. Safety Sci. Monitor 15 (2).

Le Coze, J.C., 2012. Towards a constructivist program in safety. Saf. Sci. 50, 1873–1887.

Le Coze, Jean-christophe, 2013. Outlines of a sensitising model for industrial safety assessment. Saf. Sci. 51 (2013), 187–201.

Leveson, N.G., 1986. Software safety – why, what and how. ACM Comput. Surv. 18 (2), 125–163.

Leveson, N., 1995. Safeware: System Safety and Computers. Addison Wesley Publishing Company, Reading, Massachusetts.

Leveson, N., 2004. A new accident model for engineering safer systems. Saf. Sci., 237–270
Leveson, N.G., Turner, C., 1993. "An investigation of the Therac-25 accidents". IEEE Computer, 18–41.
MISRA, 1994. Development Guidelines for Vehicle Based Software (November).
MIS-STD-882B, 1984. "System Safety Program Requirements". Department of Defense.
NASA, 1997. Software Safety: NASA Technical Standard NASASTD-8719.13A. September.
NASA Guidebook for Safety Critical Software NASA – GB-1740.13-96, 1995.
NTPC Limited, <http://www.ntpc.co.in>.
Parker, D., Lawrie, M., Hudson, P., 2006. A framework for understanding the development of organisational safety culture. Saf. Sci. 44, 551–562.
Pidgeon, N., 1998. Safety culture: key theoretical issues. Work and Stress 12 (3), 202–216.
Rasmussen, J., 1997. Risk management in a dynamic society: a modeling problem. Saf. Sci. 27 (2/3), 183–213.
Reason, J., 1998. Safety culture: some theoretical and practical issues. Work and Stress 12 (3), 202–216.
Reimann, T., Pia, O., 2007. Assessment of complex socio-technical systems – theoretical issues concerning the use of organizational culture and organizational core task concepts. Saf. Sci. 45 (7), 745–768.
Reimann, T., Pia, O., 2009. Evaluating Safety-critical Organizations – Emphasis on the Nuclear Industry. <http://www.stralsakerhetsmyndigheten.se>.
Richter, A., Koch, C., 2004. Integration, differentiation and ambiguity in safety cultures. Saf. Sci. 42, 703–722.
Starbuck, H.W., Farjoun, M. (Eds.), 2005. Organization at the limit: Lessons from the Columbia Disaster. Blackwell Publishing.
Snook, S.A., 2000. Friendly Fire, The Accidental Shootdown of US Black Hawks Over Northern Irak. Princeton University Press.
Software Considerations in Airborne Systems and Equipment Certification. DO178B 1992.
*"Software Safety"*, NASA Technical Standard, 1997 <http://satc.nasa.gov/assure/distasst.pdf>.
Vaughan, D., 1996. The Challenger Launch Decision: Risky Technology, Culture and Deviance at NASA. University of Chicago Press, Chicago.
Vaughan, D., 1999. The dark side of organizations: mistake, misconduct, and disaster. Annual Review of Sociology 25, 271–305.