Article can be accessed online at http://www.publishingindia.com

Towards Safety Assessment Checklist for Safety-critical Systems

P.V. Srinivas Acharyulu*, P. S. Ramaiah**

Abstract

Safety-critical systems are ever increasing in day to day life such as use from microwave oven to robots involving computer systems and software. Safety-critical systems must consider safety engineering and safety management principles in order to be safe when they are put into use. Safety analysis must be done. Safety assessment of such systems is difficult but not impossible. They must deal with the hazards analysis in order to reduce or prevent risks to environment, property damage and / or loss of life through risk-free and failure free or fail-safe operations. The existing methods are found to be limited and inadequate to address the risks associated and for safety assessment. This paper proposes a methodology for safety assessment of safety critical systems based on identifying significant and non-significant aspects of risk. The methodology considers various contributions towards risk and safety assessment. The methodology reviews existing risk categories and classification. This paper also presents a set of risk contributing factors and significance denoting function. A case study of typical power plant operations for safety assessment is presented to validate proposed methodology. The methodology provides clarity to improve safety of safety-critical systems. This paper also discusses about the scope of automation. The results indicated that substantial increase in risk ranking with the proposed methodology to that of existing risk ranking indicating the safety assessment.

Keywords: Safety-Critical Systems, Functional Safety, Software Safety, Software Quality, Safety Automation

1. Introduction

Safety-Critical Systems are those systems whose failure could result in loss of life, significant property damage, or damage to environment (Knight, J.C, 2002). Safety in broad pertains to the whole system, computer hardware, software, other electronic & electrical components and stake holders. A safety-critical system is such a system which has the potential to cause hazard either directly or indirectly. The emphasis of this paper is on the element of software for such safety critical systems, which can be referred to as safety critical software. Some of the safety critical applications include flight control systems, medical diagnostic and treatment devices, weapon systems, nuclear power systems, robots and many. Failure free and risk free or fail-safe operations may not lead to hazards. Thus safety is dependent on correct operation of such systems when these systems are automated or computerized. Each of such software should have specific purpose with adequate safety and additional relied capabilities to be realized while in operation. Exhaustive study and analysis of hazards is must to integrate safety through computerization in safety automated systems. Hazards related to whole system, circumstances in which the system has to operate, hardware and software components have to be elucidated. Software becomes accountable for hazards if it causes hazard and can be referred as hazardous if used to control / monitor hazard. A strong risk assessment with respect to whole system, hardware and software is required by studying impacts and their aspects.

Some examples of Safety Critical Systems are *Defense* - Weapon Delivery Systems, Space Research Programs,

* Research Scholar, Department of Computer Science & Engineering, GITAM University, Visakhapatnam, Andhra Pradesh, India. E-mail: pvschari@gmail.com

** Professor, Department of Computer Science and Systems Engineering, College of Engineering, Andhra University, Visakhapatnam, Andhra Pradesh, India. E-mail: psrama@gmail.com

Production Industries – Production and Manufacturing controls, Maintenance, and 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 etc

Some examples of automation technologies include, Automation Systems, Identification Systems, Human Controlled Systems, Industrial Controls, Industrial system Controls, Service Specific Requirement Systems, Sensor Systems, Power Control Systems, PC based automation etc.

2. Safety Related Terms

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 ((Medikonda, 2009).

Error: An incorrect internal system state (Medikonda, 2009).

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, 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 (MIL STD 882C, 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 (MIL STD 882B, 1984). A real-time system is safety critical when its incorrect behavior can directly or indirectly lead to a state hazardous to human life (MIL STD 882C, 1984). Decisions which shape the software architecture for safety-critical, real-time systems are driven in part by three qualities namely availability, reliability and robustness (MIL STD 882C, 1984) (NASA Tech Std., 1997).

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 (MIL STD 882C, 1984).

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 (MIL STD 882C, 1984).

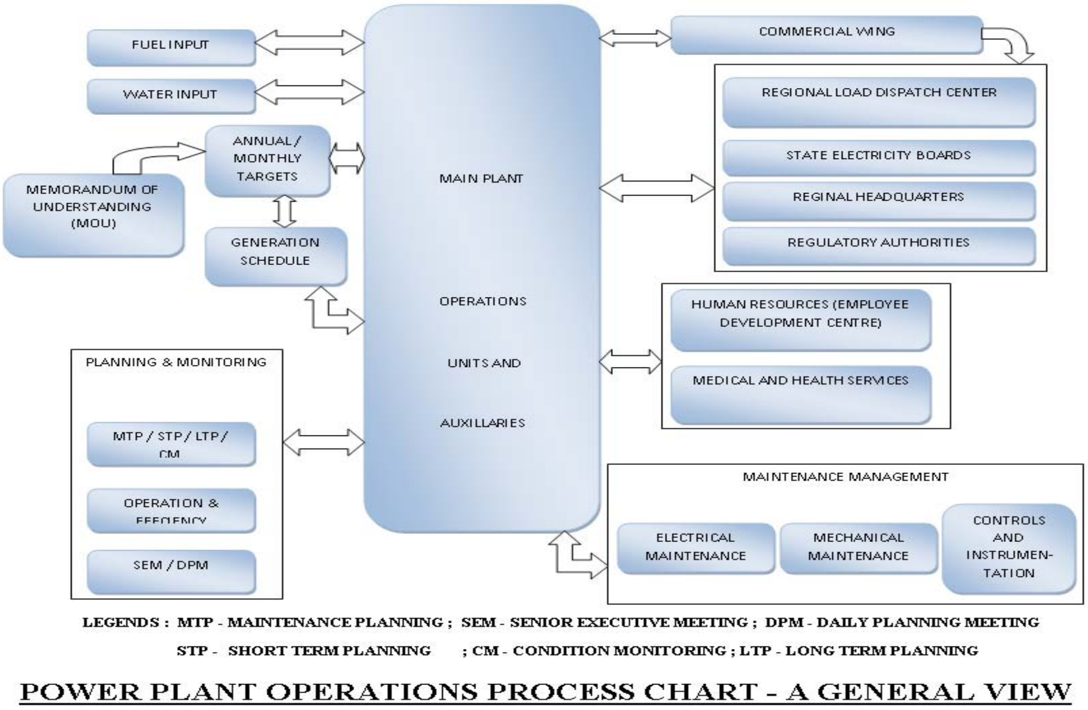
3. Power Plant System Life Cycle

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:

i. Safe and Efficient Operation of the Units
ii. Effective re-commissioning after Overhauling (OH)
iii. Effective start-up and shutdown as per the guidelines
iv. Organizing safety talks for awareness
v. Ensure usage of Personal Protective Equipments (PPEs)
vi. 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 in coordination and compliance with the planning, derived requirements, statutory guidelines and in accordance with the law and standards.

Figure 1: Block Diagram of Power Plant Operations (NTPC)


FUEL INPUT
WATER INPUT
ANNUAL / MONTHLY TARGETS
MEMORANDUM OF UNDERSTANDING (MOU)
GENERATION SCHEDULE
PLANNING & MONITORING
MTP / STP / LTP / CM
OPERATION & EFFECIENCY
SEM / DPM
MAIN PLANT
OPERATIONS
UNITS AND
AUXILLARIES
COMMERCIAL WING
REGIONAL LOAD DISPATCH CENTER
STATE ELECTRICITY BOARDS
REGINAL HEADQUARTERS
REGULATORY AUTHORITIES
HUMAN RESOURCES (EMPLOYEE DEVELOPMENT CENTRE)
MEDICAL AND HEALTH SERVICES
MAINTENANCE MANAGEMENT
ELECTRICAL MAINTENANCE
MECHANICAL MAINTENANCE
CONTROLS AND INSTRUMEN-TATION
LEGENDS : MTP - MAINTENANCE PLANNING ; SEM - SENIOR EXECUTIVE MEETING ; DPM - DAILY PLANNING MEETING
STP - SHORT TERM PLANNING ; CM - CONDITION MONITORING ; LTP - LONG TERM PLANNING
POWER PLANT OPERATIONS PROCESS CHART - A GENERAL VIEW

3.1. System Operational Constraints

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 comprising 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 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.

3.2. Safety Critical Functions

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. This process involves chemistry, occupational health and safety issues.

Safety Critical Operations 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 environmentally, legally, health & safety, equipment robustness, and proper budget utilization if safety critical operations are not planned or fail in proper risk assessment. Maintenance involves electrical, mechanical, civil, controls and instrumentation engineering areas, contributes to maintain equipment for safe operations, safety of people working with and to environment. If these maintenance works are not carried in a systematically planned as per planning & monitoring schedules, decisions may contribute to accidents.

3.3. Other Functionalities

Human Resource & Employee Development Center (HR & EDC) activities include utilization of allocated budget for Corporate Social Responsibility (CSR) for conducting welfare activity in the surrounding villages, medical camps, 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. Report 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.

4. Generic Safety Life Cycle

A functional generic safety flow process works on a specific design flow in accordance with the statutory guidelines in an industry. It comprises the following phases relevant to specific field. First a safety process area shall be identified such as aviation, transportation, operation, maintenance, and the like. Depending on the selected area of incorporating safety measures planning suitable to the area shall be adopted, and feasibility study will be undertaken, leading to the identification of critical systems incorporated within the industry. Risks and hazards analysis shall be carried out, deriving to form safety requirements.

Further deepening into the risks and hazards analysis, depending on the classification of hazards, appropriate measures of mitigation or prevention, elimination, reduction, or alternative needs be incorporated, and then measurements done before and after adopting to control measure. Evaluations are carried out before and after control measures. Once the system passes through all phases, necessary documentation of the activity, compliance with the standards stipulated shall be verified and validated. Otherwise, repeated review and audit is carried out until successful compliance is achieved.

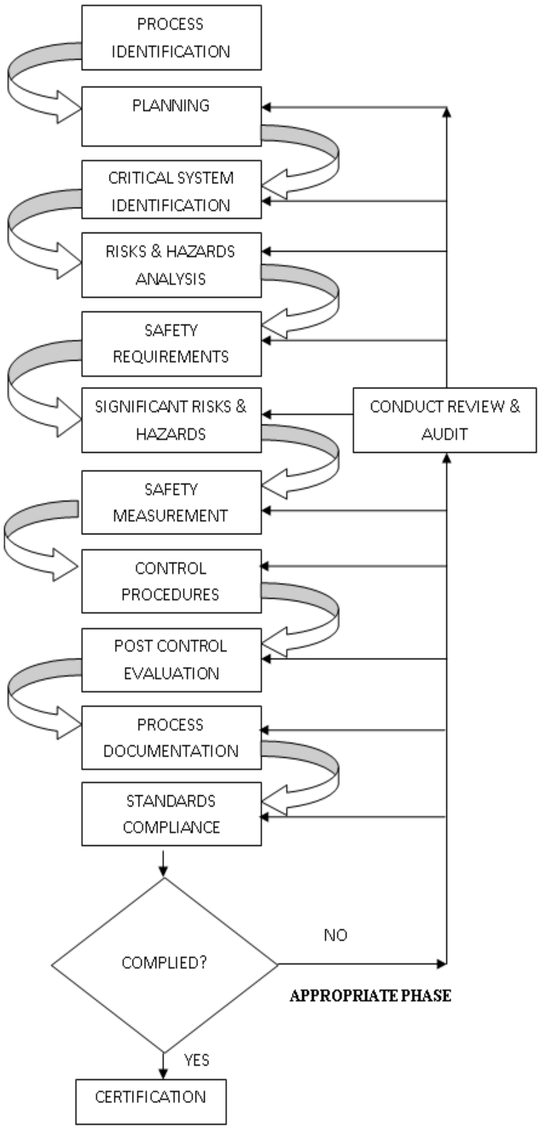
5. Scope of Automation

Safety automation specific to the area of safety critical function and some example such technologies includes

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 involves computer hardware and software, whether may be electrical, electronic or mechanical. 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 and 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.

Figure 2: Generic Safety Life-Cycle



The design and development of Integrated Safety Management Information System (ISMIS) with reference to the activities specified in section 3.1 through 3.3 basing on the proposed methodology would definitely escalate the needy areas of safety attention.

6. Proposed Methodology for Safety Assessment

The tasks involved in the proposed methodology are

1. Risk Aspects Identification
2. Operating Conditions Identification
3. Risk Likelihood Identification
4. Risk Detectability Identification
5. Risk Consequence Identification
6. Identification of significant operations
7. Risk Categorization
8. Safety Adequacy Measure Identification
9. Risk Assessment and Evaluation
10. Design & Development of ISMIS

6.1. Risk Aspects Identification

In broad, various risk aspects identified in safety critical system operations are classified as shown in the following table 1. Appropriate risk ranking may be given for the aspect based on the operations of safety critical activity.

Table 1: Risk Aspects and Description

Code	*Description / Meaning*
AP	Air Pollution
WP	Water Pollution
WEP	Work Environment Pollution
LC	Land Contamination
NP	Noise Pollution
RL	Resource Loss / Revenue Loss
L	Legal
FH	Fire Hazard
OHS	Occupational Health & Safety
CSR	Corporate Social Responsibility
RD	Radiation

6.2. Conditions Identification

It has been identified that safety critical systems functions in various conditions. They are shown in table 2 below. Risks are associated with and depend on the nature of activity and involve humans, environment and property. Relevant risk ranking can be assigned with the priority of condition.

Table 2: Classification of Operations

Code	Condition	Description/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

6.3. Risk Likelihood Identification

Risk likelihood probability is shown in table 3. Likelihood of risk bears an impact on determining the significance of hazard. Relevant risk rank determines and directs the safety management to initiate suitable action to mitigate risk.

Table 3: Probability of Risk Likelihood

Code	Description / Meaning	Risk Rank
DL	Definitely Likely	10
VHL	Very Highly Likely	9
HL	Highly Likely	8
MHL	Moderately High	7
MML	Moderately Low	6
LL	Likely Low	5
VLL	Very Low Likely	4
RCL	Remote Chance of Likely	3
VRCL	Very Remote Likely	2
ANL	Very Highly Un-Likely	1

6.4. Risk Detectability Identification

Risk detectability greatly contributes to safety and determines the significance of activity. Relevant risk rank is assigned so as to prioritize the safety measures specific to the safety critical activity. Detectability coding, meaning and relative risk ranks are shown in table 4.

Table 4: Risk Detectability

Code	Description / Meaning	Risk Rank
HI	Highly Impossible	10
VR	Very Remote	9
R	Remote	8
VL	Very Low	7
L	Low	6
M	Moderate	5
MH	Moderately High	4
H	High	3
VH	Very High	2
AD	Almost Detectible	1

6.5. Risk Consequence Identification

Risk consequence identification specific to a safety critical operation plays very important role in determining the safety level of operation by it risk rank of hazard occurrence. Consequence coding, meaning and relative risk ranks are shown in table 5

Table 5: Risk Consequence and Coding

Code	Description / Meaning	Risk Rank
HS	Hazard Sudden	10
HW	Hazard with Warning	9
VH	Very High	8
HH	High Hazard	7
MH	Moderately High	6
LH	Low Hazard	5
VLH	Very Low	4
MH	Minor Hazard	3
VMH	Very Minor Hazard	2
NH	No Hazard	1

Table 6: Hazard Significance Indicator

Code	*Meaning / Units*	*Risk Level Weight (Wt)*		
		Measurement	*Intensity*	*Wt*
E	Extent / Area	< 0.5 km	Low	1
		>=0.5km & < 3km	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 to 60 Minutes	Medium	2
		>= 60 Min	High	3
RL	Resource / Revenue Loss	< 100000	Low	1
		>=100000	Medium	2
		>= 5000000	High	3

6.6. Identification of Significant Operations

Significance of any safety critical operation depend on five parameters namely extent of hazard, intensity, frequency, duration and resource/revenue loss. Each factor is further identified with three degrees as low, moderate and high. Appropriate risk rank of 1, 2 and 3 are assigned to calculate significance where safety attention to be explored. Significance is the product of assigned weight of risk rank for each of the parameter. Thus the highest risk rank would be 243 and lowest would be 1. These are shown in table 6 below.

Significance = E * I * F * D

6.7. Risk Categorization

Risks are categorized into six levels, such as discomfort, minor injury, reportable major injury, permanent disability. Discomfort which is momentary and minor injury as it is recoverable or an acceptable consequent risk can be treated as negligible risk and thus given the lowest & lower risk level. While a reportable risk is treated as moderate, thus medium risk level is assigned. Consequences of major injury and permanent disability are designated as strong category and hence assigned high level risk rank. Finally highest risk rank is assigned for potential risk category when they lead to consequences of fatalities or catastrophic effects.

6.8. Safety Adequacy Measure Identification

The following table 8 shows identified safety adequacy measure and applicability of computers for automating safety protecting systems.

Table 7: Categories of Risks

Category Code	*Class*	*Description / Meaning*	*Risk Rank*
C1	Negligible	Discomfort	1
C2	Negligible	Minor Injury	2
C3	Moderate	Reportable	3
C4	Strong	Major Injury	4
C5	Strong	Permanent Disability	5
C6	Potential	Fatal or catastrophic	6

6.9. Risk Assessment and Evaluation

Risk assessment is calculated as sum of severity and detectability. Severity is the product of likelihood and consequence, denoted as follows

Table 8: Safety Adequacy Measures

Code	*Description / Meaning*	*Safety Adequacy Measure*
AP	Air Pollution	Automated Air pollution detection Systems, personal protective equipments
WP	Water Pollution	Chemical Analysis and detection
WEP	Work Environment Pollution	Automated Systems
LC	Land Contamination	Automated garbage collection and removal systems
NP	Noise Pollution	Excess Noise detection systems and protective equipments
RL	Resource Loss / Revenue Loss	Austerity measures
L	Legal	-
FH	Fire Hazard	Fire safety control systems, sensors, alarms etc
OHS	Occupational Health & Safety	Appropriate medical diagnostics and treatment
CSR	Corporate Social Responsibility	Educating, creating safety awareness and adoption of villages
RD	Radiation	Excessive radiation detection systems, protective equipments

Risk = Severity + Detectability

(Severity = Likelihood X Consequence)

Accordingly each of the safety critical activity through design and development of integrated safety management information system reports significant risk according to the levels of risk and facilitate in adapting appropriate safety activity measure to handle risks

6.10. Design & Development of ISMIS

The design and development of Integrated Safety Management Information System (ISMIS) with reference to the activities specified in section 3.1 through 3.3 basing on the proposed methodology would definitely escalate the needy areas of safety attention. Relevant databases with the risk ranking pertaining to each of the safety critical tasks to be carried out and information provided by the ISMIS in a wide range of reporting and elucidating safety requirements. The permutations and combinations of risk aspects would facilitate management to take appropriate safety measure and risk reducing remedies. During long term it will much flexible to monitor incidents, evaluation of safety tasks that have been carried out to mitigate risks for each of the safety critical activity or product or service, such that safety attention can be prioritized for next consecutive safety life cycle.

7. Application of Methodology to a Case

The methodology is applied to a case of safety-critical power plant operations of fuel handling systems for validation. The following results indicated that substantial increase in risk assessment there by reducing the overall safety index, implying requirement of safety attention. The aspect of work environment pollution (WEP) is taken into consideration.

Overall Safety Index can be calculated as

X = Total No. of Operations = 75

Y = Total No. of Safety-critical operations = 35

OSI = Overall Safety Index = (Y/X)*100

= (35 / 75) * 100

= 46.6 %

Absolute Safety Level Index is calculated as

P = Significant Safety-Critical Operations = 6

Q = Total No. of Safety-Critical Operations = 35

SA = (P/Q)*100

= (6 / 35) * 100

= 17.14 %

Table 9: Results Obtained for WEP Aspect

Serial No	Description	Value / (%)
1.	Total No. of Operations	
2.	Total No. of Safety Critical Operations	
3.	No. of Safety Critical Operations Per aspect	
4.	No. of Significant Safety Critical Operations	
5.	Determine Significance 5.1. Hazard Extent 5.2. Hazard Intensity 5.3. Hazard Frequency 5.4. Hazard Duration	
6.	No. of Significant Hazardous Operations	
7.	No. of Significant Non-Hazardous Operations	
8.	Determine Risk category (C1/C2/C3/C4/C6)	

8. Conclusion

This paper presented various risk aspects related to different contexts, operating conditions, identified advanced level likelihood, consequences, detectability, significance determinants, categorized risks with their class and suggested safety adequacy measures with respect identified risk aspects. The paper presented a ten point scale, for likelihood, consequence, detectability and significance denoting function which forms the basis for safety assessment. The scope of automation has also discussed and some of the examples were given.

Those safety-critical functions indicated in section 3.2, if fails may contribute to hazards relevant to that aspect. For example, chemical analysis of raw material for quality involve in chemistry may result in release of toxic gases and exposure in the environment leading to consequences to humans working in and around with varying dimensions. Automation systems can be adopted in order to improve safety with addition safety adequacy measures indicated in table 8. Integrated Safety Management Information system is designed and developed to assess risk with above proposed methodology indicated satisfactory results. The methodology provided clarity to improve safety critical operations leading to enhance safety to humans, environment and property. This work requires further extension to address implementation costs and time. More rigorous work is needed to meet the complete set of requirements.

References

1. Dunn, W. R. (2003). Designing Safety Critical Computer Systems. Published by the IEEE Computer Society 0018-9162/03/$17.00 © 2003 IEEE (pp. 40-46).
2. IEEE 100, *The Authoritative Dictionary of Standard Terms*. IEEE Press 2000.
3. IEC, International Standard, Functional Safety of Electrical/ Electronic/Programmable Electronic Safety- Related Systems–IEC 61508-3. Part 3 Software Requirements. (1998).
4. Knight, J. C. (2002). *Safety Critical Systems: Challenges and Directions*. Proceedings of the 24th International Conference on Software Engineering (pp. 547-550) Orlando, Florida.
5. Kumar, S. P., Ramaiah, P. S. & Khanaa**,** V. (2009). A Methodology for Modeling Software Safety in Safety-Critical Computing Systems. *International Journal of Computer Science and Network Security*, July, 9(7), 185-193.
6. Lawrence, J. D. & Preckshot, G. G. (1994). Design Factors for Safety-Critical Software. Retrieved from http://www.llnl.gov/tid/lof/documents/pdf/228132.p
7. Leveson, N. (1995). *Software: System Safety and Computers*. Massachusetts: Addison Wesley Publishing Company, Reading.
8. Leveson, N. G. (1986). Software Safety-Why, What and How. *ACM Computing Surveys*, June, 18(2), 125-163.
9. Leveson, N. G. (2004). The role of software in spacecraft accidents. *Journal of Spacecraft and Rockets*, 41(4), 564-575.
10. Leveson, N. G. & Turner, C. (1993). An investigation of the Therac-25 accidents. *IEEE Computer*, July, 26(7), 18-41.
11. Medikonda, B. S. & Panchumarthy, S. R. (2009). A framework for software safety in safety-critical systems. Retrieved from http://doi.acm.org/10.1145/1507195.1507207. DOI: 10.1145/1507195.1507207
12. MIL-STD-882C. (1984). *System Safety Program Requirements*. Department of Defense.
13. MIS-STD-882B. (1984). *System Safety Program Requirements*. Department of Defense.

14. MISRA. (1994). Development Guidelines for Vehicle Based Software.

15. NASA Technical Standard. (1997). *Software Safety. Retrieved from http://satc.nasa.gov/assure/distasst.pdf*

16. NTPC Limited: A Government of India Enterprise. Retrieved from *http://www.ntpc.co.in*

17. Software considerations in airborne systems and equipment certification. DO178B (1992).