Production Management and Process Control, Vol. 104, 2023, 1–7
https://doi.org/10.54941/ahfe1003046

Plant Engineer Performance Improvement for Effective Risk Reduction

Hiroshi Ujita and Naoko Matsuo

Institute for Environmental & Safety Studies, Tokyo 171-0042, JAPAN

ABSTRACT

To reduce the risk in the complex systems, it must be firmly suppressed in the original design process, so the safety concept is thoroughly incorporated into the system based on risk management at the design stage before operation. Next step, implement risk reduction measures are considered based on risk management at the construction or operation stages. As a response to the problem that remains even after taking measures in advance, that is, a risk that occurs at the stage of using equipment or processes, failure or error is detected by cause analysis and the countermeasure is taken. As countermeasures, it is the most important to give feedback to the hardware, next to software, and when it is not possible, it is important to take countermeasures by the organization or team, not to blame the individual fault. In summary, it is necessary to enhance performance for dealing with problems that are anticipated in advance, and then to enhance error detection that remains even after setup. There are six reduction activities to reduce risks. One is effective use of human performance tools as Tool-box Meeting during runtime, and another is cause analysis as 5 why when the problem occurred. While effective risk reduction must be realized in the planning phase, in which there are four type of risk management activities; risk assessment by practical engineers at the field work planning, long-term issue consideration cleared by the feedbacks from various risk assessments in the plant and understood by executives, risk analysis on the safety system and maintenance activities on the usual system. Four risk reduction measures are the key for risk management in the plant: hazard reduction itself, occurrence frequency reduction by preventive measures, consequence reduction by installing mitigation systems, and by mitigating operation.

Keywords: Risk management, Defense in depth, Risk reduction, Risk analysis, Cause analysis, Human performance improvement, Human characteristics

INTRODUCTION

Inflexible or unchangeable organization is clearly supposed to include fatal risk in the system under current highly and fast developing situation, no matter how its size is. It means that any system doesn't reach the best results even if anyhow behaviour's done, being not adjustable for risk reduction, due to variety and change in the system design or the organization decision-making. Namely, the Key for "the most rational optimization along with keeping the development" is actualized by using risk management adjustable

to all organization or system, to solve the complicated issues struggling in current fast-changing international situation.

Risk management concept is the most important philosophy for improving the safety of the huge complex system. Every engineer knows well and always considers about "The local optimization would make the entire worst", and therefore well-balanced design and operation are required [1]. Even the total safety has been assured by the safety design based on Defense in Depth concept [2], operational problem would occur in the future by the chain of the fallacy of the Defense in Depth, then safety culture degradation, and finely organizational accident eventually happened. Probabilistic approach is required to the problems. In addition to this, we should answer to the question of "Safety Goal: How safe is safe enough?" to acquire the public confidence. Risk assessment is required to respond to the local optimization and operational problems, and to safety goal question.

Risk management in a huge complex system is an activity that aims to improve safety by the balanced system without excess or deficiency by design (hardware / software) and operation (human) [3]. In other words, it is the risk reduction activities giving the top priority to the risk concept. At present, the existing huge complex systems have been reduced in hardware / software risk through its countermeasures and quality assurance activities based on safety logic, so the remaining risk can be said to be an event involving humans. For this reason, risk reduction activities can be described as human, that is plant engineer, performance improvement activities. Furthermore, continuing this activity will eventually lead to the improvement of the safety culture. In other words, what we want to emphasize here is that "risk management", "risk reduction activities", "human performance improvement activities", and "improvement of safety culture" have similar purposes and contents.

RISK REDUCTION STEP

It must be firmly suppressed in the original design process, so the safety concept is thoroughly incorporated into the system based on risk management at the design stage before operation. Next step, implementation of risk reduction measures is considered based on risk management at the construction or operation stages. As a response to the problem that remains even after taking measures in advance, that is, a risk occurring at the stage of using equipment or processes, activity step to reduce the risk in the operation phase must be required as described in Fig. 1. Following three steps are the effective risk reduction measures: First in the planning phase, risk analysis and countermeasures are taken, second during runtime, effective use of Human Performance Improvement tools, and third when the problem occurred, that is a failure or error is detected, cause analysis as 5 why is performed and the countermeasure is taken [4-5]. We will first under-stand the vulnerabilities at the time of implementation and the weaknesses in human relationships between organizations and teams. As countermeasures, it is most important to give feedback to the hardware, next to software, and when it is not possible, it is important to take countermeasures by the organization or team, not to blame the individual. Measures against human errors are implemented by

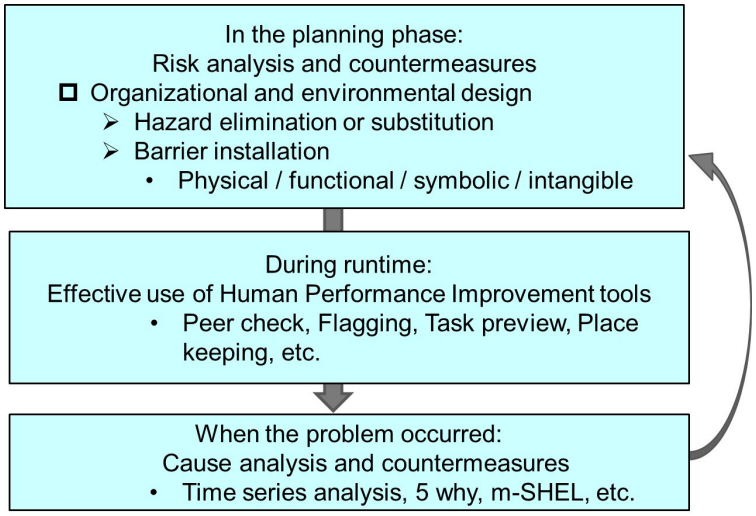

Figure 1: Risk reduction activity step.

the devices and the mechanisms rather than the discipline. In summary, it is necessary to enhance performance for dealing with problems that are anticipated in advance, and then to enhance error detection that remains even after setup.

EFFECTIVE RISK REDUCTION ACTIVITIES IN PLANNING PHASE

Effective use of human performance tools during runtime and cause analysis when the problem occurred are of course important activities for risk reduction, while effective risk reduction must be realized in the planning phase, in which there are four type of risk management activities as shown in Table 1.

First, risk assessment by practical engineers at the field work planning, especially for the job situation at the first time, after a long time, or when job change. Second, on the contrary, consideration on long-term issues cleared by the feedbacks from various risk assessments in the plant and understood by executives, such as social issues or organizational culture problems. Remaining two are issues concerned about plant system risk assessment. Third, risk analysis, which evaluates random failures or human errors, to determine surveillance test interval on the safety system (stand-by system). Fourth one is maintenance activities on the usual system based on failure physics, such as risk-informed in-service-inspection. Risk matrix must be utilized in risk evaluation or risk control stage. Characteristics of total six approaches are completely different each other, and then sections to respond for them, such as safety, maintenance, quality assurance personnel, executives, etc., are also different, that is risk reduction activities can be achieved by all members efforts in the plant.

RISK REDUCTION MEASURE

In general, a system has functions of hardware (mechanical / electric / electronic system) and software (control system). Hazard that threatens the safety

Table 1. Risk reduction activities in plant.

System risk reduction phase			Risk evaluation *	Risk control * (Examples)	Responsible section
Planning	Field work		Risk assessment at field work planning	For the first time, After a long time, When changing	Each section
	Plant system	Safety system (Stand-by system)	Risk analysis (Random failure/ human error)	Surveillance test interval	Safety section
		Usual system	Maintenance activities based on failure physics	Risk-informed in-service-inspection	Maintenance section
	Long-term issues		Feedbacks from various risk assessments	Social Issues/ Organizational culture	Executives
Runtime			Leveraging human performance improvement tools	Review on plan by field survey	Safety/ Maintenance section
Problem occurred			Cause analysis	Feed back to design/ operation	Each section/ QA section

of the system lies anywhere in the lifecycle which com-posed of planning, concept development, design, manufacturing, operation, maintenance, and disposal phases of the system. Therefore, it is difficult to achieve high safety only by fragmentary safety technology, post-mortem analysis, engineering safety evaluation focusing on hardware, or safety evaluation focusing only on human factors during operation. In particular, huge complex systems and products sold in large volumes can cause enormous losses and tragedies in the event of an accident. To improve risk management, preventive risk management analysis is essential. It analyses the hazard risks (thorough pre-analysis and evaluation) over the life cycle of the system and drafts control measures (safety design that removes and controls hazards) to keep the risks below target levels, derived by Safety Goal in advance. Risk matrix is effectively used for decision in both steps.

Figure 2 explains the concept of risk reduction measure. There are many measures illustrated in 'Risk curve', such as hazard itself reduction, frequency reduction effectively achieved by prevention, and consequence reduction by mitigation. Systems installed for reducing risk in huge complex system plant have capability to reduce not only consequence but also frequency as illustrated in 'Event tree'. If the measures successfully performed consequence must be reduced, while failed, frequency reduced.

Table 2 summarize risk reduction measures for various systems, which are the key processes for risk management in plant. There are four methods to reduce risk. One is hazard (poisoning by accident onto residents) reduction itself, such as change to small plant size or attach intrinsic safety features, which is very difficult because it must change the design concept itself. Second is occurrence frequency reduction by preventive measures, installing barriers

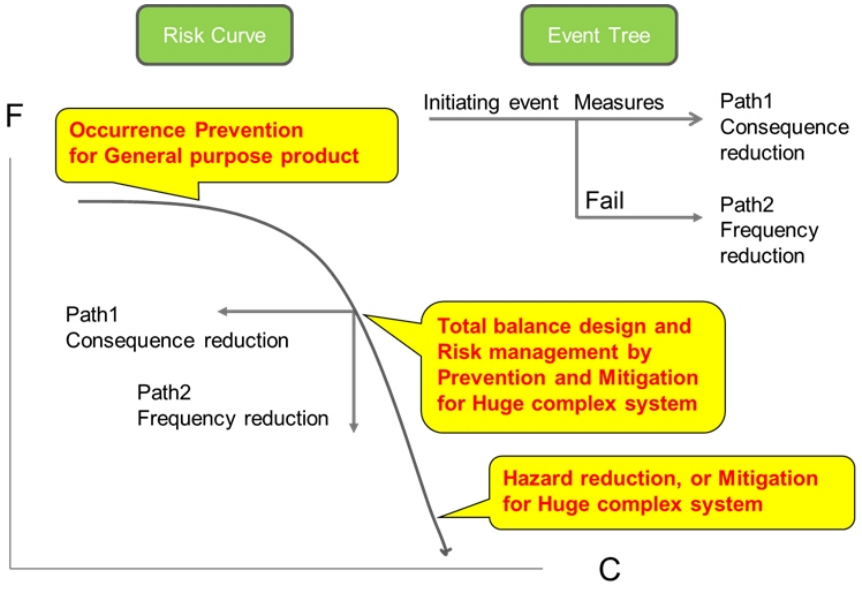

Figure 2: Concept of risk reduction measure.

Table 2. Risk reduction measures for various systems.

System		Hazard (Risk source) / Object	Risk reduction measure			
			Hazard reduction itself	Occurrence frequency reduction by preventive measures	Consequence reduction	
					Mitigation system	Mitigating operation
Natural hazard		Typhoon Earthquake / Public	Out of control	Out of control	Flood control (dams, embankments), Earthquake resistance	Migration, Evacuation
Huge complex system	Transport system	Collision, Overturn, Crash/ Passenger	Change to small system size or attach intrinsic safety features	Barriers, Safety logic	Softening equipment ·Seat belt	Evacuation, Postponement
	Plant system	Poisoning by accident / Resident	Change to small plant size or attach intrinsic safety features	Barriers, Safety logic, safety systems	Mitigation system or incident planning	Emergency planning, Evacuation
		Poisoning during usual operation / Resident	Change to small plant size or attach intrinsic safety features	Barriers Safety logic, safety systems	Stable operation	Distance
General-purpose products		Injuries, Burns, Electric shock/ Consumer	Replacement	Safety design	Safety cover	Manual
Industrial accident		Drop, Collision, Injury, Burn, Electric shock/ Worker	Automation, Alternative work	Barriers (foolproof, failsafe)	Safety equipment (cloth, belt, helmet, shoes)	Manual, Rule

such as safety logic or safety systems, etc. Third is consequence reduction by installing mitigation system or incident planning, etc. Fourth is consequence reduction by mitigating operation such as emergency planning, evacuation, etc.

As the case of natural hazard as Typhoon, Earthquake, etc., occurrence of natural hazard cannot control, and then flood control such as dams or embankments, or earthquake resistance are installed when countermeasures are ineffective, migration or evacuation will be considered. Take countermeasures to reduce risks of safety critical system as transport system or plant system is the most critical mission. The transport system such as aviation system or railway system considers only safety operation. While the plant system such as chemical plant or nuclear power plant considers not only safety operation but also accident response. Countermeasures for general-purpose products adopts simple ones. Industrial accidents occur anywhere and then both prevention and mitigation are taken.

Four countermeasures take completely different methodologies each other, and then we must select the most effective way by discussions from designers to operators, from practical engineers to executives, that is effective risk reduction measures can be realized by all members efforts in the plant.

CONCLUSION

Risk management concept is the most important philosophy for improving the safety of the huge complex system. Every engineer knows well and always considers about "The local optimization would make the entire worst of the system", and therefore understands importance of the risk management concept that well balanced design and operation are required. At present, the existing huge complex systems have been reduced in hardware risk through hardware countermeasures and quality assurance activities based on safety logic, so the remaining risk can be said to be an event involving human factors. For this reason, risk reduction activities can be described as plant engineer performance improvement activities.

To reduce the risk in the complex systems, it must be firmly suppressed in the original design process, so the safety concept is thoroughly incorporated into the system based on risk management at the design stage before operation. Next step, implementation of risk reduction measures is considered based on risk management at the construction or operation stages. As a response to the problem that remains even after taking measures in advance, that is, a risk occurring at the stage of using equipment or processes, following three steps are the effective risk reduction measures: First, in the planning phase, risk analysis and countermeasures are taken, second during runtime, effective use of Human Performance Improvement tools, and third when the problem occurred, that is a failure or error is detected, cause analysis such as 5 why is performed and the countermeasure is taken. Effective risk reduction must be realized in the planning phase, in which there are four type of risk management activities. First, risk assessment by practical engineers at the field work planning. Second, on the contrary, long-term issue consideration cleared by the feedbacks from various risk assessments in the plant and understood by executives. Third, risk analysis on the safety system. Fourth one is maintenance activities on the usual system. Total six approaches have completely different methodologies each other, and then sections to respond

for them, such as not only safety, maintenance, or quality assurance personnel, but also executives, etc., are also different, that is risk reduction activities can be achieved by all members efforts in the plant.

Risk reduction measures are the key for risk management in the plant. There are four methods to reduce risk. One is hazard reduction itself, such as change to small plant size or attach intrinsic safety features etc. Second is occurrence frequency reduction by preventive measures, installing barriers such as safety logic or safety systems, etc. Third is consequence reduction by installing mitigation systems. Fourth is consequence reduction by mitigating operation. We must select the most effective way by discussions from designers to operators, from practical engineers to executives, that is effective risk reduction measures can be realized by all members efforts in the plant.

ACKNOWLEDGMENT

The work was supported in part by the member of the committee in Japan Nuclear Safety Institute, to establish the concept of human performance improvement based on risk management in order to create its lecture course for plant engineers.

REFERENCES

IAEA, 'Defense in Depth in Nuclear Safety, INSAG-10, A report by the International Nuclear Safety Advisory Group', 1996.

Ujita, H., Maeda, N., Kurabayashi, M: "Improvement of human performance in risk management" course' (1)–(3), The 63rd Annual Conference of the Japan Ergonomics Society, 2022.7 (In Japanese).

Ujita, H., Matsuo, N.: 'Human Performance Improvement Activities for Risk Reduction', AHFE2022, 2022.7, New York.

Ujita, H., Matsuo, N.: 'System Safety, Risk Management, and Human Performance Improvement', HCI2020, 2020.7, Virtual.

USDOE, Human Performance Improvement Handbook, Volume 1&2, *DOE*-HDBK-1028-2009.