A Fresh Look at Barriers from Alternative Perspectives on Risk

Xue Yang*, Stein Haugen

Norwegian University of Science and Technology, Trondheim, Norway

Abstract: This paper takes a fresh look at alternative perspectives on major accident causation theories to highlight the fact that these perspectives can supplement and improve the energy barrier perspective. The paper starts from a literature study of energy barrier perspective, Man-Made Disaster theory (MMD), Conflicting Objective Perspective (COP), Normal Accident Theory (NAT), High Reliability Organization theory (HRO), Resilience Engineering (RE), and System-Theoretic Accident Model and Processes (STAMP) model to find out main concepts and identify critical factors. A further study of safety barrier perspective is carried out using STAMP methodology to understand how barrier functions can fail. It was found that alternative perspectives can supplement the barrier perspective by structurally analyzing possible failure causes for barrier function (STAMP, MMD), looking for driving forces for unsafe decisions and unsafe actions when human interacts or be part of barrier systems (COP, HRO), and emphasizing possible complex interactions and tight coupling within barrier functions (NAT, RE). Furthermore, suggestions to barrier management based on best practices from these perspectives are presented, which will be developed into concrete risk reduction measures, such as checklists, audits schemes, or indicators to help decision-makers better comprehend and maintain the performance of barrier functions in further work.

Keywords: Accident causation, Barriers, STAMP, HRO, Resilience Engineering, Safety management

1. INTRODUCTION

Over the past decades, safety gains increasing interests among industries to prevent loss of lives, economical loss and adverse consequences to the environment due to major accidents. Parts of the reasons are high-visibility accidents that resulted in tragedies and significant environmental damage all over the world, such as Three Mile Island accident, Ocean Ranger sinking, Chernobyl disaster, Piper Alpha disaster, Texas city refinery explosion, Deepwater horizon oil spill, etc.

Motivated by the desire to understand deeply what causes accident and how to prevent major accidents, various accident causation theories have been developed. Each accident theory has its own characteristics based on causal factors it highlights [1]. The energy-barrier perspective [2, 3] emphases on energy flow control and mitigation of consequences caused by release of energy based on a defense-in-depth principle. Man-Made disasters theory [4-6] highlights lack of information flow and misperception among individuals and groups during an incubation period. Conflicting objectives perspective [7] looks into driving forces for unsafe decisions that push systems towards safety boundary. Normal Accident Theory [8] is a rather pessimistic perspective stating that major accidents are inevitable in complex systems due to "*interactive complexity*" and "*tight coupling*". System-Theoretic Accident Model and Processes (STAMP) [9] perceives accident causation from a systemic viewpoint, indicating that accidents arise from inadequately enforced safety constraints, flawed control process and inconsistent, incomplete or incorrect process model. High Reliability Organization (HRO) [10, 11] and Resilience Engineering (RE) [12-14] perspectives, which aim at building up a robust organization, focus on a series of properties of organization that can contribute to avoid major accidents. Strictly speaking, HRO and RE are not accident causation models. However, due to their important implications to accident prevention, they are also covered in this paper.

Among these seemingly competing perspectives, the energy-barrier perspective is the most popularly applied accident causation theory in Norwegian Oil and Gas industry. This is mainly due to huge

* Tel.: +47 73 59 71 05; fax: +47 73 59 28 96.
E-mail address: xue.yang@ntnu.no

amount of energy that is handled in the industry and disastrous consequences of major accidents to human lives, environment, and economical losses. Subscription of one perspective doesn't mean denying others. Rosness, Grøtan [15] compared these perspectives (except STAMP) and concluded that they are complementary, rather than contradictory to each other. After all, most of these perspectives are conceptualizations of common characteristics of past accidents that have significant implications for future major accident prevention. The purpose of this paper is to take a fresh look at these perspectives, to highlight the fact that these alternative perspectives can supplement and improve the energy-barrier perspective from different angles. The following research questions are discussed in detail in the rest of the paper.

1. What are the main concepts and principles of these perspectives?
2. How can they contribute to supplement and improve the energy-barrier perspective?
3. What are the implications for safety management?

This paper is mainly based on a study of above alternative perspectives of major accident causation theories, with a special focus on barrier perspective. The remainder of this paper is organized as follows. In section 2, main principles of alternative perspectives are summarized with a focus on critical causal factors that they emphasize. In section 3, differentiation between *barrier function* and *barrier system*, analysis of possible flaws in *barrier function* are carried out as necessary steps before utilizing essences from alternative perspectives to improve the barrier perspective. In section 4, implications to safety management are discussed and section 5 concludes the work.

2. MAIN PRINCIPLES OF DIFFERENT PERSPECTIVES

2.1. Energy-Barrier Perspective

Energy-barrier perspective is widely applied in Norwegian oil and gas industry. Barrier perspective origins from energy model that was introduced by Gibson [3] and further popularized by Haddon [2] with ten strategies for accident prevention. The basic idea is that accidents occur when control of dangerous energy is lost and there are no effective barriers between the energy source and vulnerable assets. [2]. This is the classical interpretation of barrier. The hazard control strategies are commonly referred as defense-in-depth principle. This was further developed by the "Swiss cheese model" which shows how an accident emerges due to holes in multiple barriers [16] caused by *active failures* and *latent conditions*. The concept of "barrier" is further extended into process model, as a means to prevent transitions between accident developing phases. The extended barriers are not only related to energy anymore, but also radically interpreted as "a physical and/or nonphysical means planned to prevent, control or mitigate undesired events or accidents [17]". Energy-barrier perspective is further discussed in Section 3.

2.2. Man-Made Disaster Theory (MMD)

Man-Made disaster theory suggested that disasters can be systematically analyzed rather than thinking them as "acts of god" or chance events that have nothing in common [5]. The theory shifted the focus from engineering calculation of reliability to soft factors that lead to failures. Turner's essential conclusions based upon a systematic qualitative analysis of 84 British accident inquiry reports over ten years were:

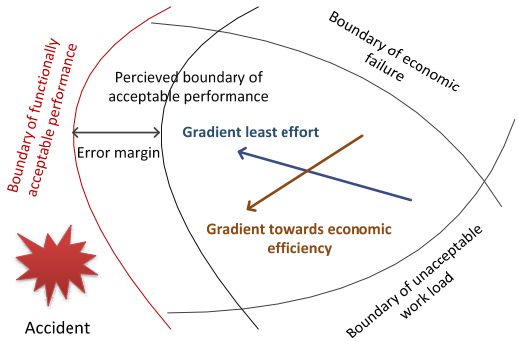
- Accidents or disasters develop through a long chain which is called the *incubation period*. The *incubation period* is characterized by the "accumulation of an unnoticed set of events which are at odds with the accepted beliefs about hazards and the norms for their avoidance [5]".
- Accidents arise from an interaction between human and organizational arrangements of the socio-technical systems set up to manage complex risk problems
- The build-up of latent errors and unnoticed events is accompanied by a collective failure of organizational cognition and intelligence

Dekker [18] pointed out that this *incubation period* is the most fascinating time where "drifts" are happening and accumulated that end up with a surprise of failure. Why a set of drifts or accumulated drifts are not noticed is because of rigidities of belief, misperception of danger signals, or simply events are unnoticed or are misunderstood. The root causes of the *incubation period* are generalized as *lack of information flow* and *misperception among individuals and groups*.

2.3. Conflicting Objective Perspective (COP)

The conflicting objectives perspective (COP) explains the driving forces behind "bad" safety related decisions by pointing out that accidents are caused by a systematic migration of organizational behavior under the influence of pressure toward cost-effectiveness in an aggressive, competitive environment [7]. The danger is that safety may gradually be sacrificed to economic and workload pressures, consciously or unconsciously. The closeness to the acceptable risk boundary determines the degree of proneness to accident (Figure 1).

Figure 1 Boundaries of Safe Operation. Adapted from Migration Model [7]



Rasmussen [7]'s migration model raises the need for identification of boundaries of safe operation to better control risk. To handle conflicting objectives, it is crucial to make boundaries visible and touchable, and to develop concrete coping skills at the boundaries. One way is to increase awareness of the boundary using instructions and motivation campaigns to create a counter gradient to the cost-effectiveness gradient to maintain the margin [7]. The biggest challenges are then: 1) how to identify where the boundaries are, and 2) how to make them visible to decision makers?

2.4. Normal Accident Theory (NAT)

The key idea suggested by NAT is that "major accidents are inevitable due to "*interactive complexity*" and "*tight coupling*" in complex systems [8]. Perrow [8] defined *complex interactions* as "those in which one component can interact with one or more other components outside of the normal production sequence, either by design or not by design". He further explained the definition of *Interactive complexity* in the preface of his new book in an more understandable way as [19]: "*Interactive complexity* is not simply many parts; it means that many of the parts can interact in ways no designer anticipated and no operator can understand. Since everything is subject to failure, the more complex the system the more opportunities for unexpected interactions of failures." *Tight coupling* means "there is no slack or buffer or give between two items" [8]. The *tight coupling* can happen to space, schedule, or resource. The tightness of coupling indicates how fast cause and effect can propagate through the system.

2.5. High Reliability Organization (HRO)

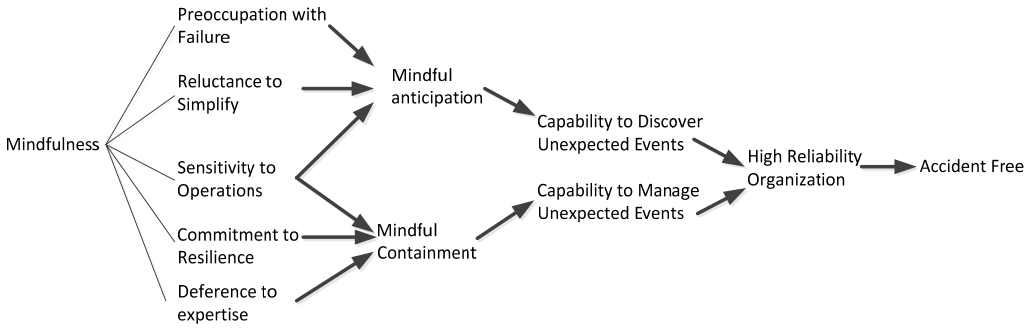
HRO research was initiated about 20 years ago and identified several characteristics that maintained the safety of the studied organizations [11, 20, 21]:

- Deference to expertise during emergencies

- Management by exception: managers monitor decisions but do not interfere unless there is a clear unplanned deviation in a course of action
- Climate of continuous training
- Several channels are used to communicate safety critical information
- In-built redundancy include back-up systems, internal cross-checks and continuous monitoring of safety critical activities

There has been much debate in HRO theories regarding whether to define and identify a HRO based on accident statistics or on the processes that it uses to successfully manage the risks [11, 20, 22, 23]. The focus of HRO research has changed to the types of processes and practices that enable certain organizations to achieve a safe state. One representative work is from Karl Weick, who conceptualized HROs as "mindful" organizations which highlights what an organization needs to do to achieve a continuous safe state [24]. *Mindfulness* is more about inquiry and interpretation grounded in capabilities for action [25]. The key messages of Weick and Sutcliffe [26] is to create a *mindful infrastructure* that continuously maintain HRO principles: preoccupation with failure; reluctance to simplify; sensitivity to operations; commitment to resilience; and deference to expertise (Figure 2).

Figure 2 HRO Principles Summarized from Weick and Sutcliffe [26]



2.6. Resilience Engineering (RE)

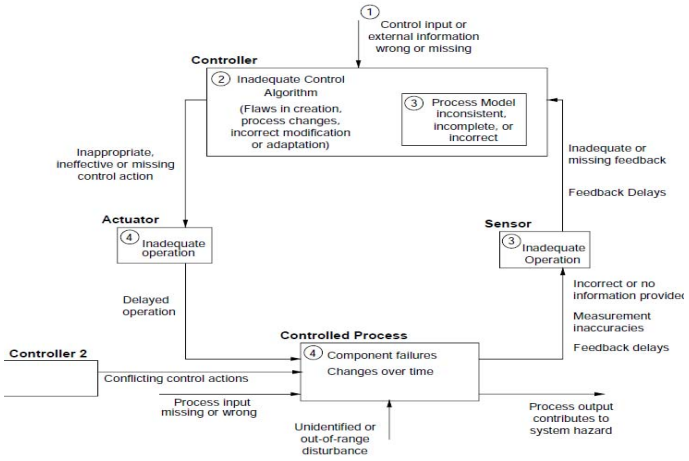
A key concept in Resilience Engineering is that safety is not "freedom from unacceptable risk" anymore, but the "ability to succeed under varying conditions" [12]. Resilience is a family of related ideas, instead of one single thing [27]. Hollnagel first defines resilience as "the ability of a system or an organization to react and recover from disturbances at an early stage, with minimal effect on the dynamic stability" in the first volume of Resilience Engineering Perspectives series [14]. Woods [14] considers resilience as a wider capability more than adaptability. This definition emphasizes the *robustness* of the system. This means resilience is concerned with unanticipated perturbations, which arise because of the incomplete, limited or wrong competence envelope, or environmental changes so that new demands/pressures/vulnerabilities arise that undermine the effectiveness of the competence measure in play. Therefore, Woods argues that resilience engineering must monitor the boundary conditions and adjust or expand the model to accommodate changes. These boundaries are called textbook competence envelope, which is relative to unanticipated perturbations. Hollnagel provided a more elaborate working definition in the second volume to address other than adaptability [13], which was repeated in the third book [12] as "the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions". This definition expanded resilient reactions to changes, in addition to disturbances. Meanwhile, *robustness* under unexpected conditions is further emphasized. But somehow the "ability to recover" is diluted. This simplifies resilience into ability to dynamically steering activities, under both expected and unexpected conditions. Mattila, Hyttinen [28] defining '*managerial resilience*' based on findings from oil industry, interviews with offshore managers who had faced serious emergencies, showed that their trade-off decisions were key to maintaining the safety of installation. This is exactly what conflicting objective perspective is talking about. So Resilience , as a family of related ideas [27], seems to be a collection of at least barrier perspective,

conflicting objective perspective, and HRO theories [29], with the aim of achieving safe state by *dynamically and wisely steering activities*.

2.7. System-Theoretic Accident Model and Processes (STAMP)

Leveson [30] conceives safety as a control problem and accidents arise from flawed processes; interactions among people, societal, and organizational structures, engineering activities, and physical system component. This is in line with Rasmussen's framework for risk management that addresses Structural hierarchy and System dynamics [7]. STAMP consists of three basic constructs: *safety constraints*, *hierarchical control structure*, and *process models*. Correspondingly, accidents can be studied by identifying which safety constraints were missing or violated or inadequately enforced; how inadequate control happened; and whether process model is inconsistent, incomplete or incorrect (Figure 3).

Figure 3 Possible Flaws in Control Loop that May Lead to Hazards [9]



3. ENERGY-BARRIER PERSPECTIVES AND ALTERNATIVE PERSPECTIVES

The energy-barrier perspective is popularly applied in offshore oil production platforms, as a result of huge amount of energy involved. The scenarios of release of hydrocarbons and defense-in-depth barriers are modelled in sequence. The underlying assumption is that accidents happen because of absence or breach of these barriers. Subscription of one perspective does however not mean others are not applicable. The Snorre A blowout accident that had been analyzed from alternative perspectives (except STAMP), shows that each perspective tells a part of the story [15]. In order to see how other perspectives can supplement and improve barrier perspective in a systematic way, we need to see how barriers are working to prevent, control and mitigate unwanted outcomes first.

3.1. Barrier Function and Barrier System

Under energy-barrier perspective, it is useful to distinguish between *barrier function* and *barrier system*. *Barrier function* is "a function planned to prevent, control, or mitigate undesired events or accidents", while *barrier system* is "a system that has been designed and implemented to perform one or more *barrier functions*" [17]. Therefore, the *barrier function* is realized or executed by one or multiple *barrier systems*. These *barrier systems* are maintained or modified to maintain the desired *barrier function* during operation. The main focus in traditional offshore quantitative risk analysis (QRA) is on technical safety systems. However, the performance of *barrier systems* that are modelled in QRA may be far away from the real performance of *barrier function* during operation. BOP is one of the examples. OLF 070 [31], a widely followed guideline in the Norwegian oil and gas industry, requires that the Probability of Failure on Demand (PFD) of Blowout Preventer (BOP) as a *barrier system* should be between 10^{-3} and 10^{-2}. However, in practice, it was found only the 6 out of 11 cases

on deep-water rigs that pushed the activation button of the BOP actually brought the well under control [32]. This means that BOP used by deep-water rigs as a *barrier function* had a "failure" rate of 45%, instead of between 0.1% and 1%.

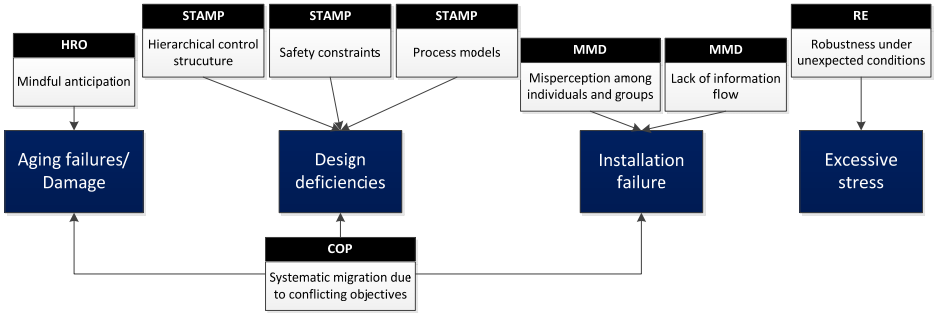
3.2. Types of Barrier Systems and Alternative Perspectives

Barrier system may be classified according to several dimensions depending on the purpose of classification, as discussed in Sklet [17]. Our purpose is to identify different working mechanisms of *barrier systems* to see how other perspectives can influence their functions. Therefore the dimension from Hollnagel [33] that divide barrier systems into *physical (or material), functional (active or dynamic), symbolic* and *incorporeal* is selected for further discussion.

3.2.1. Physical (or material) barrier system

Physical barrier systems passively stand after installation to withstand forces up to a certain maximum beyond which it is no longer effective. Physical barrier systems are normally simple, passive systems. Some examples are fire walls, cages, explosion-proof container, and so on. The performance of these systems during operational phase is rather good and stable. Possible failures of the *barrier systems* could be: aging failures/damages, design deficiencies, installation errors, and excessive stress that beyond design limits [34]. When we dig further to find causes from alternative perspectives, STAMP provides possible explanations for design deficiencies: safety constraints are missing, violated or inadequately enforced throughout the hierarchical control structure; unmatched process model between designers and real situation. Installation failures, such as wrong location and wrong type of materials, are not uncommon in the field. This may happen due to insufficient information flow among designers and installation personnel. Aging failures, which can most possibly be avoided by scheduled proactive maintenances, maybe traced back to insufficient mindful anticipation that miss out early symptoms of degraded systems at early stage. Excessive stress, which means operational environment exceeds textbook competence envelope of the systems, is one type of *unanticipated perturbations* in RE which need more robust design to conquer. Conflicting objectives can be a reason behind aging failure, design deficiencies, and installation failure due to cost or schedule pressure. Above failure causes from alternative perspectives are summarized and structured in Figure 4.

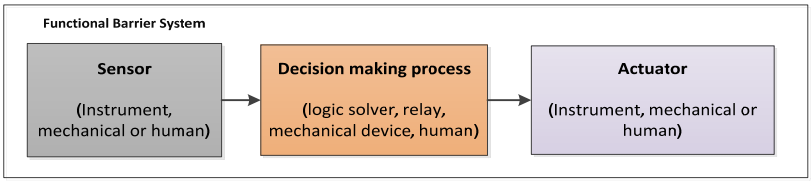
Figure 4 Failure Causes of Physical Barrier System and Alternative Perspectives



3.2.2. Functional barrier system

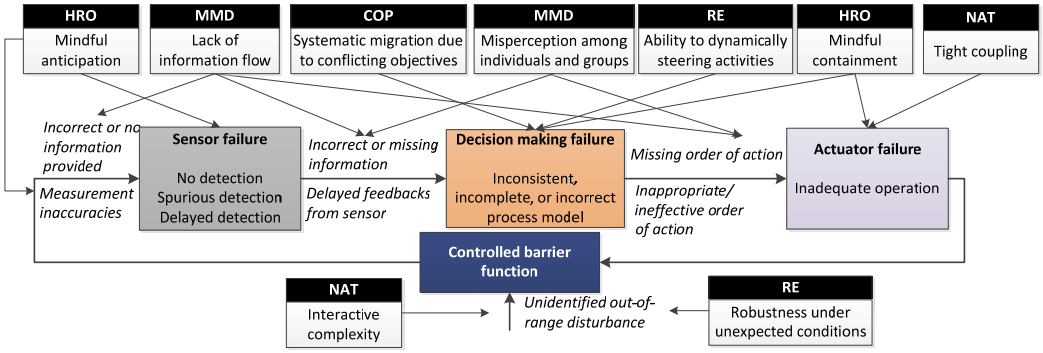
Functional barrier systems are active and can be activated when one or more pre-set conditions are met. Pre-designed actions will be carried out after a decision-making process. These systems vary from simple systems (e.g. interlock) to complex system (e.g. Safety Instrumented Systems), from technical systems to human operations. The three elements that are involved in the functional barrier system are sensor, decision making process and actuator (Figure 5). The performance of the systems becomes unreliable when human beings play the three roles

Figure 5 Key Elements in Functional Barrier System Adapted from [35]



Since there is generally a process involved in the systems, the STAMP control framework (Figure 3) is adopted to identify possible flaws in the *barrier function*. We can see from Figure 6 that in addition to technical failures that may be caused by factors illustrated in Figure 4, more possible causes for failed barrier functions can be identified: information flow in between; inconsistent, incomplete, or incorrect process model (algorithm); inadequate/no operation; and unidentified out-of-range disturbance. When humans are involved in the *barrier function*, which mean humans are the ones to detect, make decision, or act upon, the failure causes become more complicated. After all, interaction failure between humans and machines has been realized as the largest contributor to the probability of system failure [36].

Figure 6 Possible Flaws in Controlled Barrier Function Executed by Functional Barrier System



Human as sensors - Human has more flexibility than technical sensors. This has both positive and negative effects. When the pre-set condition is satisfied, there may be no output from the "sensor" due to: 1) we intentionally refuse to acknowledge that we know, is even by sub-consciousness. 2) Prior information is noted but not fully appreciated 3) Prior information is not correctly assembled 4) Relevant information is available, but when it is in conflict with prior information, rules or values, it is neglected and not taken into discussion [4]. The ability to "sense" is the essence of "*mindful anticipation*" in HRO perspective. This requires operators to be preoccupation with failure, reluctance to simplify, and sensitivity to operations.

Human as decision-makers - With respect to decision-making process, automated systems have basically static control algorithms, with periodic updates when necessary. In contrast, humans employ rather dynamic control algorithms, which can be easily influenced by other factors. Many process safety barriers need human's action like pressing Emergency Shutdown button to activate *barrier function*. Normally, it is a call about when to push the button. "Too late" activation of last defense barrier has appeared in several accident investigation reports [37]. Conflicting objectives due to high workload or cost pressure may prevent operators from making sound and timely decisions, consciously or unconsciously. The gap between operator's process model and real condition is a major cause for wrong decisions. In the Deepwater Horizon blowout accident, when Well Integrity Test was carried out to test cement casing, operators believed that as long as the pressure in the kill pipe is 0, based on U-tube effect principle, the integrity of the well can be verified. This process model is wrong. The fact is that the kill pipe was not in communication with the water-filled cavity below so that U-tube was not actually established [37]. Being aware of flaws in the process model, *dynamically*

steering activities from RE and *mindful containment* from HRO contribute significantly to avoid failure of barrier function.

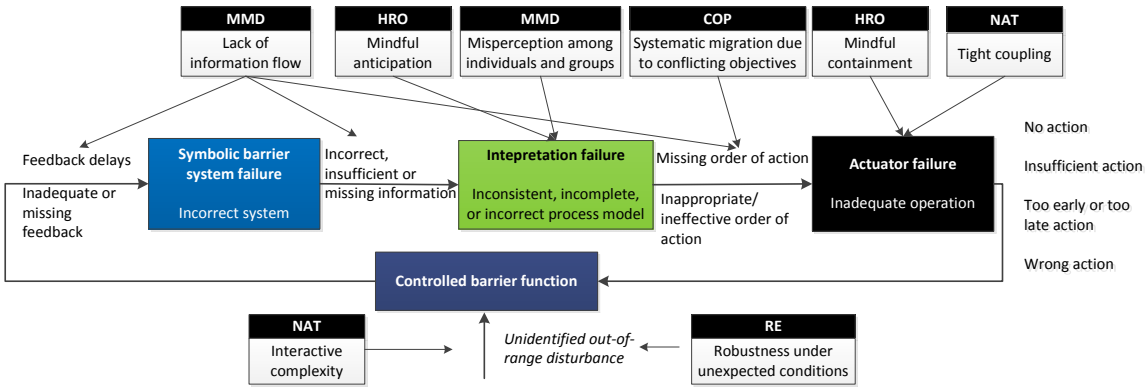
Human as actuators - Human is not a pump that can do a controlled start or stop following command. Commission failures, including violations, mistakes, slip and lapses, can happen when human act as an actuator [38]. The reasons behind might be *tight coupling* in terms of schedule, space or resource, or lack of *mindful containment*.

Unidentified out-of-range disturbance - Out-of-range disturbance is not part of barrier system or barrier function. The ideal design is supposed to cover all the possible situations the barrier system may face. We have to acknowledge it is impossible for designers to foresee everything. Handling disruptions and variations that fall outside the base mechanisms is addressed in NAT in terms of interactive complexity and Resilience Engineering in terms of unanticipated perturbations. Imaginations, learning from experience, early detection, close monitoring, and dynamically steering activities are proposed by RE to reduce the influence from out-of-range disturbance to the least degree [14, 39].

3.2.3. Symbolic barrier system

Road signaling system, signs, procedures, work permit, belong to this category. Symbolic barrier systems themselves cannot complete *barrier function*. Instruction, procedure, work permit cannot prevent any unwanted outcome from happening. It is the interpretation and action that complete the barrier function (Figure 7). Obviously, a road sign of speed limit of 50 only works when drivers notice them and actually slow down the speed under the limit. Symbolic barrier system is sometimes considered at the same level of efficiency, strength and robustness as functional barrier system or physical barrier system, which is generally not the case in practice [40].

Figure 7 Possible Flaws in Controlled Barrier Function Executed by Symbolic Barrier System



Comparing to functional barrier systems, the feedback loop that is addressed in STAMP and HRO deserves more attention to keep a symbolic barrier system reliable and effective. This is a weak link during operation. Vicente, Mumaw [41] found out that in nuclear power plants, where tasks and procedures are strictly prescribed, violations of instructions or skipping of steps have been repeatedly observed. On one hand, the behavior of operators appears to be quite rational given the actual high workload and time constraints. On the other hand, this reflected the deficiencies in the procedures themselves that need to be reported and improved. This is the same to warnings and signals. In spite of the great efforts putting into developing early warnings, many warnings are ignored and eventually accidents happened. A shift supervisor who worked in control room for Three Mile Island 2 nuclear power plant testified that there had never been less than 52 alarms lit in the control room and it had been a habit to ignore most of the alarms [42]. This is mainly due to the unreasonable design. User experience of these procedures and warning systems need to be reported and continuous improvement need to be implemented to bridge the gap between symbolic barrier systems and the practice.

3.2.4. Incorporeal barrier system

These barrier systems are largely synonymous with so called organizational barriers, i.e. rules that are imposed by the organization rather than being physically, functionally or symbolically present in the system, laws, safety culture, knowledge and skill [43]. Safety culture [16, 44] as a representative incorporeal barrier system, aims at building a foundation so that the designers and operators' can have 'good' safety beliefs, attitudes. Their behaviors are expected to act as additional accident barriers [45]. This is basically what HRO is talking about under *mindful infrastructure*. Another type of incorporeal barrier system is rules, laws and restrictions. This is emphasized in STAMP under concept of *safety constraints*, and Rasmussen's socio-technical framework. Enforcement of safety constraints sufficiently and adequately to lower levels in a hierarchical safety control structure, and finally implement to actions are the keys to utilize incorporeal barrier system.

4. IMPLICATIONS FOR SAFETY MANAGEMENT

Under a radical interpretation of barriers, all kinds of functions, elements and systems that are associated with safety are given the label "barrier" [40]. This created confusions and illusion that as long as we have a sufficient number of barriers in place, we are safe. The fact is that different types of barrier systems have different levels of adequacy, response time, effectiveness, specificity, reliability, robustness and independence. Discussions in section 3 illustrated that alternative perspectives can supplement the energy barrier perspective by structurally analyzing possible failure causes for barrier functions (STAMP, MMD), looking for driving forces for unsafe decisions and unsafe actions (COP, HRO), and emphasizing possible complex interactions and tight coupling among barrier systems (NAT, RE). In this section, the implications and suggestions to safety management of barriers are made to better manage *barrier functions* other than technical failures.

1. *Make sure the selected barrier system is optimal – No cost or workload pressure*

Realization of barrier function starts from selection of *barrier systems*. Generally speaking, physical and functional barrier systems are more effective and reliable than symbolic and incorporeal barriers, whereas resources required are much higher [43]. For instance, writing a new procedure is a common risk reduction measure as it is a quick and inexpensive way to implement [15]. Therefore, whether the barrier system selection is under economical or production pressure needs to be checked when designing the barrier systems.

2. *Periodically test and maintain information flow in technical functional barrier system*

For technical functional barrier systems, failure modes other than technical failures need to be identified and countermeasures have to be designed. The information flow among sensors, decision-making process, and actuator must be periodically tested and maintained. Barrier system doesn't equal to complete barrier function, especially for human functional barrier system and symbolic barrier system. This means further efforts are needed when these two types of barrier systems are selected.

3. *Check and enhance capability of human sensors*

When humans interact within functional barrier systems as sensors, we should enhance the capability of discovering unexpected events, require operators to be preoccupied with failures, avoid simplifications, and improve sensitivity to operations. Detecting deviations is not as straightforward as it looks. Make clear definitions and increase awareness of the deviations and abnormalities among operators; encourage raising of doubts and questions; treat all unexpected events as important information; develop sceptics; speak up [26]; all these needs organization to build up a culture fertilizer so that mindful behaviors and conscious inquiry [27] can grow.

4. *Facilitate sound decisions by efficient information management, accurate process model, relevant indicators and "safety first" mind*

When humans interact as decision-makers, make sure that the safety margin is not squeezed by the decision before taking any further action is crucial. "Deference to expertise" is necessary, but at the same time, we have to remember also centralization plays an important role to understand the big

picture. Sound decision depends upon sufficient, high quality, timely information. Systematic efforts are needed to build up efficient information management system. To facilitate decision-making process, we would need to identify indicators of the developing incubation period. Accurate process model needs continuous feedbacks, learning from past experience, training and knowledge sharing [26].

5. Reduce chances of human errors when they act as actuators

When human interact as an actuator, the key is to make sure the person fully acknowledges and understood the "mission", and reduce the chances for human error due to competence, disposable work descriptions, governing documents, technical documentation, design, Human Machine Interface (HMI), communication, supervision, time pressure, workload, work motivation, and attitude failures [38]. Organizational redundancy can be implemented as another barrier to detect the deviations of action from the "actuator" if necessary.

6. Emphasis on interpretation, action and feedback channel while using symbolic barrier systems

Effective symbolic barrier systems heavily rely on action and feedback channel. The gap between procedure and practice needs to be bridged by continuous feedbacks and updating. Design of signals and warnings has to be reasonable and practicable. Otherwise they could be counter-productive and speed up the development of accidents. These require robust reporting systems, comprehensive safety information systems, and rapid response [9].

7. Build up strong safety culture and sufficiently enforce safety constraints to reinforce incorporeal barrier systems

Incorporeal barrier systems are not physically present. Safety culture is the shared cognitions and administrative structure rather than individual attitudes to safety that deserves to be studied for development of organizational understanding regarding to risk and danger [4]. Four facets promoted by 'good' safety culture are: senior management commitment to safety; shared care and concern for hazards and solicitude over their impacts upon people; realistic and flexible norms and rules about hazards; and continual reflection upon practice through monitoring, analysis and feedback systems (organizational learning). For the other type of incorporeal barrier systems in terms of laws, restrictions, the enforcement of these safety constraints needs "vertical" alignment across the levels as indicated in social-technical framework [7] and Leveson's sociotechnical control model [30].

8. Keep in mind of "anticipated perturbations" and "interactive complexity"

There is textbook competence envelope for every barrier system. Anticipated perturbations and interactive complexity are unavoidable during operation. Monitoring boundary conditions and dynamically steering activities under both expected and unexpected conditions are required to accommodate changes.

5. CONCLUSION AND FURTHER WORK

Safety management on barriers has been focused on technical failures of physical and functional barrier systems. Along with extension from energy-oriented barriers to unwanted outcome-oriented barriers, barrier's performance during operational phase becomes unreliable due to human's interaction. The paper improves the understanding of how barrier functions can fail in terms of different types of barrier system. The possible failure modes of barrier functions identified in section 3.2 can be used as a guide to design and follow the performance of barrier systems. It was found that alternative perspectives on major accident provide explanations for possible flaws that exist in barrier functions and countermeasures from design to operation. This result testified the conclusion from Rosness, Grøtan [15]: these perspectives are complementing each other instead of competing. Furthermore, STAMP and barrier perspectives are conceived to be two totally different ways of risk modelling approach since STAMP is based on safety constraints emphasizing dynamic control, while barrier perspective is based on events (i.e. barrier failures) [30] which is rather static. Using STAMP methodology to model barrier function executed by functional barrier system and symbolic barrier system revealed its potential to systematically analyze how barrier functions can fail, such as how

unsafe decision can be made and where information flow deficiency can happen. The applicability of possible flaws in controlled barrier function frameworks (Figure 6 and 7) need to be tested in case studies. However, this still opens the door to further research on how to manage barriers dynamically during operational phase.

Suggestions to better management of barriers are made from best practices of reviewed perspectives. Some suggestions are still quite conceptual and general that need to be further developed into concrete risk reduction measures, such as checklists, audits schemes, or indicators that can help decision-makers better comprehend and maintain the performance of barrier functions.

References

[1] Kjellén, U., *Prevention of accidents through experience feedback*. 2002: CRC Press.

[2] Haddon, W., *The basic strategies for reducing damage from hazards of all kinds.* Hazard Prevention, 1980.

[3] Gibson, J.J., *The contribution of experimental psychology to the formulation of the problem of safety-a brief for basic research*. 1961, New York, Association for the Aid of Crippled Children.

[4] Pidgeon, N. and M. O'Leary, *Man-made disasters: why technology and organizations (sometimes) fail.* Safety Science, 2000. **34**(1–3): p. 15-30.

[5] Turner, B.A. and N.F. Pidgeon, *Man-Made Disasters*. 1997: Butterworth-Heinemann Limited.

[6] Turner, B.A., *Causes of disaster: sloppy management.* British Journal of Management, 1994. **5**(3): p. 215-219.

[7] Rasmussen, J., *Risk management in a dynamic society: a modelling problem.* Safety Science, 1997. **27**(2–3): p. 183-213.

[8] Perrow, C., *Normal accidents: Living with high risk technologies*. 1999: Princeton University Press.

[9] Leveson, N., *Engineering a Safer World: Systems Thinking Applied to Safety (Engineering Systems)*. 2012: The MIT Press.

[10] Laporte, T.R. and P.M. Consolini, *Working in practice but not in theory: Theoretical challenges of "high-reliability organizations"*. Journal of Public Administration Research and Theory, 1991. **1**(1): p. 19-48.

[11] Roberts, K.H., *Some characteristics of one type of high reliability organization.* Organization Science, 1990. **1**(2): p. 160-176.

[12] Hollnagel, E., et al., *Resilience engineering in practice: A guidebook*. 2011: Ashgate Publishing, Ltd.

[13] Hollnagel, E., C.P. Nemeth, and S. Dekker, *Resilience engineering perspectives: remaining sensitive to the possibility of failure*. Vol. 1. 2008: Ashgate Publishing, Ltd.

[14] Hollnagel, E., D.D. Woods, and N. Leveson, *Resilience Engineering (Ebk) Concepts and Precepts*. 2006: Ashgate Publishing.

[15] Rosness, R., et al., *Organizational accidents and resilient organizations: six perspectives*. 2010, SINTEF Technology and Society.

[16] Reason, J.T. and J.T. Reason, *Managing the risks of organizational accidents*. Vol. 6. 1997: Ashgate Aldershot.

[17] Sklet, S., *Safety barriers: Definition, classification, and performance.* Journal of Loss Prevention in the Process Industries, 2006. **19**(5): p. 494-506.

[18] Dekker, S., *Drift Into Failure: From Hunting Broken Components to Understanding Complex Systems*. 2011: Ashgate Publishing Company.

[19] Perrow, C., *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters (New in Paper)*. 2011: Princeton University Press.

[20] Roberts, K.H., *Cultural characteristics of reliability enhancing organizations.* Journal of Managerial Issues, 1993: p. 165-181.

[21] Rochlin, G.I., *Defining "high Reliability" Organizations in Practice: A Taxonomic Prologue*, in *New challenges to understanding organizations*, K.H. Roberts, Editor. 1993: New York: Macmillan. p. pp. 11-32.

[22] Hopkins, A., *The problem of defining high reliability organisations.* National Research Center for Occupational Safety and Health Regulation. January, 2007.
[23] La Porte, T.R., *High reliability organizations: unlikely, demanding and at risk.* Journal of Contingencies and Crisis Management, 1996. **4**(2): p. 60-71.
[24] Weick, K.E. and K.M. Sutcliffe, *Managing the unexpected: assuring high performance in an age of complexity*. 2001: Jossey-Bass.
[25] Eede, G., W. Muhren, and B. Walle, *Organizational learning for the incident management process: Lessons from high reliability organizations.* Journal of Information System Security, 2009. **4**(3): p. 3-23.
[26] Weick, K.E. and K.M. Sutcliffe, *Managing the unexpected: Resilient performance in an age of uncertainty*. 2nd ed. 2007: John Wiley & Sons.
[27] Westrum, R., *A typology of resilience situations*, in *Resilience engineering : concepts and precepts*, E. Hollnagel, D.D. Woods, and N. Leveson, Editors. 2006, Ashgate Publishing Limited. p. 35-41.
[28] Mattila, M., M. Hyttinen, and E. Rantanen, *Effective supervisory behaviour and safety at the building site.* International Journal of Industrial Ergonomics, 1994. **13**(2): p. 85-93.
[29] Hopkins, A., *Issues in safety science.* Safety Science, 2013(0).
[30] Leveson, N., *A new accident model for engineering safer systems.* Safety Science, 2004. **42**(4): p. 237-270.
[31] OLF, *OLF 070 - Norwegian oil and gas application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry*. 2004.
[32] DNV, *Energy Report Beaufort Sea Drilling Risk Study*. 2009, Transocean Offshore Deepwater Drilling Inc.
[33] Hollnagel, E., *Barriers and Accident Prevention*. 2004: Ashgate.
[34] SINTEF, *Reliability Prediction Method for Safety Instrumented Systems - PDS method handbook 2010 edition*. 2010.
[35] Wei, C., W.J. Rogers, and M.S. Mannan, *Layer of protection analysis for reactive chemical risk assessment.* Journal of hazardous materials, 2008. **159**(1): p. 19-24.
[36] Kirwan, B., *A Guide To Practical Human Reliability Assessment*. 1994: Taylor & Francis.
[37] CCR, *Macondo The Gulf Oil Disaster. Chief Concels's Report.* 2011.
[38] Vinnem, J.E., et al., *Risk modelling of maintenance work on major process equipment on offshore petroleum installations.* Journal of Loss Prevention in the Process Industries, 2012. **25**(2): p. 274-292.
[39] Dinh, L.T.T., et al., *Resilience engineering of industrial processes: Principles and contributing factors.* Journal of Loss Prevention in the Process Industries, 2012. **25**(2): p. 233-241.
[40] Rollenhagen, C., *Event investigations at nuclear power plants in Sweden: Reflections about a method and some associated practices.* Safety Science, 2011. **49**(1): p. 21-26.
[41] Vicente, K.J., R.J. Mumaw, and E.M. Roth, *Operator monitoring in a complex dynamic work environment: a qualitative cognitive model based on field observations.* Theoretical Issues in Ergonomics Science, 2004. **5**(5): p. 359-384.
[42] Kemeny, J.G., *The need for change, the legacy of TMI: report of the President's Commission on the Accident at Three Mile Island*. 1979: The Commission.
[43] Hollnagel, E., *Risk + barriers = safety?* Safety Science, 2008. **46**: p. 221-229.
[44] Peters, G.A. and B.J. Peters, *Human error: Causes and control*. 2006: CRC Press.
[45] Taylor, J.B., *Safety Culture: Assessing and Changing the Behaviour of Organisations*. 2010: Gower.