Safety Barriers against Common Cause Failure and Cascading Failure: Literature Reviews and Modeling Strategies

L. Xie, M. A. Lundteigen, Y. L. Liu
Department of Mechanical and Industrial Engineering
Norwegian University of Science and Technology, Trondheim, Norway
(lin.xie@ntnu.no)

Abstract – **Safety barriers are required in many technical systems to reduce initiating negations, suppress failure propagations, or mitigate the consequences of common cause failures and cascading failures. Based on a thorough literature review, this paper explores the functions of safety barriers within an extended bow-tie model. The safety barriers to prevent common cause failures are important to eliminate the coupling effects on multiple components simultaneously, whereas the safety barriers against cascading failures are functional with stopping or alleviating the failure propagation by intervening coupling paths. Then, an illustrative example is introduced to demonstrate the how such two types of safety barriers are modeled and how their effects are evaluated.**

Keywords – **Safety barrier, dependent failures, common cause failure, cascading failures**

I. INTRODUCTION

Dependent failures are common in many technical systems, including railway signaling systems, safety and control systems in petroleum and chemical plants, information processing systems, and so on [1, 2]. There are a number of communication technologies and interactions between components in those technical systems. The abruptions of such systems are seldom due to single component failure, but due to some negative dependencies, e.g. miscommunications. These failures are often referred to as dependent failures.

Two sub-categories of dependent failures are of specific interest: common cause failures (CCFs) and cascading failures. Both of the two failures can occur at the same time or propagate on multiple components within a short time, leading to devastating consequences. CCFs are characterized by the simultaneous failures of two or more components due to a shared cause, while cascading failures reflect the multiple failures initiated by one component's failure that result in a chain reaction or a domino effect [3]. Many accidents demonstrate that the two kinds of the failures are great threats to technical systems. For example, CCFs are main contributors of failures in safety systems of the oil and gas industry. Some well-known accidents caused by cascading failures include fires and explosions in the chemical industry and blackouts of power grid [4, 5].

Safety barriers are introduced to prevent failures and accidents from occurring in the technical systems. Safety barriers may be physical or non-physical means to prevent, control, or mitigate negations or accidents [6]. Proper safety barriers can perform at least one of the following three safety functions against dependent failures: avoiding the initiating failures, suppressing the failure propagation, and mitigating the consequences.

Significant attention has been directed to the safety barriers that may be designed to avoid or reduce the effects of CCFs. As Smith and Watson have explained, CCFs can be found in many technical systems where redundant configurations are used to enhance system reliability [7]. Two main strategies to prevent or reduce the effects of CCFs have been proposed. One is to carry out analyses to identify and remove causes, and the other is to introduce measures to weaken the effects of CCFs. Suggested analysis methods for deploying these safety barriers may be based on cause-defense matrices, common cause analysis, and zonal analysis [8, 9]. Measures against CCFs are typically identified in design, however, the measures in the operational phase are also important [10].

Fewer researchers have focused on the effects of cascading failures compared to CCFs. A framework has been suggested by Cozzani as a basis for selecting methodology to reduce the effects of cascading failures [4]. Janssens presents a model to support the decision-making on the location of safety barriers for mitigating the consequence of cascading failures [11]. Some other researchers focus on the models for cascade control, optimization networks and implementation of mitigation cascading methods in complex networks [12-15].

Despite the efforts in identified research, it seems that few studies have focused on the differences in strategies for managing CCFs and cascading failures. It is of interest to consider efficient and suitable means to avoid or reduce effects of the dependent failures, based on deeper understanding on occurrence and propagation mechanisms of the two types of failures. We may distinguish between efforts to make each safety barrier less prone to the dependent failures, and efforts to apply safety barriers to protect the components in the technical systems against the dependent failures. This paper will focus on the latter.

The objective of this paper is to discuss the difference between CCFs and cascading failures, and safety barriers strategies to avoid or reduce the effects of the two failure categories.

The rest of the paper is organized as follows: In section 2, we discuss the basic definitions and models for dependent failures and safety barriers. Sections 3 presents an extended bow-tie model for analyzing effects of safety barriers. Examples are then employed in section 4 to illustrate the effects of safety barriers under different strategies. Conclusions and discussions occur in section 5.

II. BACKGROUND

This section explores the definitions and models regarding dependent failures and safety barriers.

A. Failures and Dependencies

IEC 60050 (191) defines a *failure* as an event when a required function is terminated [16]. A variety of classification schemes for failures has been proposed. One of them is to divide failures into independent failures and dependent failures [17]. CCFs and cascading failures are two kinds of typical dependent failures. Other dependent failures may be common mode failures (CMF), which by some communities are defined as a subcategory of CCFs and by others as a separate category. The research scope in this paper is delimited to CCFs and cascading failures.

In the guide [18] published by UK Atomic Energy Authority (UKAEA), *dependent failures* are defined as the failures whose probability cannot be expressed by the simple unconditional failure probabilities of the individual events. IEC 61508 [19] defines dependent failures as "the failure whose probability cannot be expressed as the simple product of the unconditional probabilities of the individual events that caused it".

Over the years, it has been developed a high number of models taking into account dependent failures. Dependency types and associated examples are summarized in [20] from different perspectives, ranging from physical, functional, informational, spatial to economical etc. The main approaches for analyzing dependent failures include reliability block diagram (RBD), fault tree analysis (FTA), Bayesian networks (BNs), dynamic fault trees (DFT), binary decision diagrams (BDD), Petri Nets, and Markovian models [1, 21-24].

a. CCFs

Several definitions of CCFs have been proposed in literature. IEC 61508 [19] defines a *CCF* as a failure that is the result of one or more events, causing concurrent failures of two or more separate channels in multiple channel systems. CCFs are defined by the Nuclear Energy Agency (NEA) as the dependent failures in which two or more component fault states exist simultaneously or in a short time interval, and they are direct results of a shared cause [25].

The occurrences of CCFs are always understood with their root causes and coupling factors [9, 26]. NUREG/CR-4780 [27] regards a *root cause* as the most basic reason for a component failure. A *coupling factor* refers to a characteristic of a group of components that can be susceptible to the same causal mechanisms of failures [27].

For analysis, a high number of models have been developed for CCFs. The models can be broadly classified into different groups: direct estimate models (e.g. the square-root method [28]), ratio models (e.g. β-factor model [29], C-factor model [17]), and shock models (e.g. binomial failure rate model [30]). Among them, the standard beta factor model is the most widely adopted due to its simplicity. The multiple beta-factor (MBF) model is an extension of the standard beta factor model, where a parameter account for k-out-of-n structure [31].

b. Cascading Failures

The current literature uses different names to describe cascading failures, such as induced failures, domino failures or effects, propagating errors and interaction failures [32, 33]. Murthy and Nguyen [34] consider *cascading failures* as the failures that a component's failure affects the remaining components within a system. Rausand and Høyland [3] define *cascading failures* as the multiple failures initiated by the failure of one component in the system that result in a chain reaction.

We suggest introducing the term "coupling effects" that include the concepts of coulping factors and coupling paths. The coupling effects distinghish cascading failure from the others. Coupling paths refer to paths over which coupling factors are transferred to another component [16], implying the propagation way of the cascading failures.

Several approach have been suggested for modeling the effect of cascading failures. The approaches can be categorized: topology analysis [35, 36], probabilistic risk assessment [5, 32], maintenance optimization[33, 37], and reliability analysis approaches [38]. This paper focus on reliability analysis that is a common way to measure system performanece.

B. Safety Barriers

Safety barriers are also called as countermeasures, defenses, lines of defense, layer of protection and safeguards in different regulations, standards and literatures [39]. According to a widely accepted definition, *safety barriers* are the physical or non-physical means planned to prevent, control, or mitigate undesired events or accidents [6]. Petroleum Safety Authority (PSA) of Norway emphasizes that the safety barriers should be established to reduce the possibility that errors and hazards occur [40].

Barriers functions are related to the functions planned to prevent, control, or mitigate accidents [6]. It is common to classy the barrier functions as prevention to reduce accident probability, control the deviation, and mitigation accident developments.

A lot of qualitative and quantitative approaches have been proposed for barrier analysis, such as safety barriers analysis (e.g. hazard-barrier matrices, bow-tie diagram), energy-barrier analysis (e.g. Energy flow/barrier analysis), and protection barrier analysis (e.g. Swiss cheese model, Layer of protection analysis (LOPA), barrier and operational risk analysis (BORA)) [41].

However, few of these approaches have paid attention to how efficient and suitable safety barriers may be introduced for different kind of dependent failures. That is why we propose an investigation of the potential difference in strategies to prevent or reduce the effects of CCFs and cascading failures. The research approach include three main parts: (1) Identification of inputs that are related to dependent failures and safety barriers; (2) Development of extended bow-tie model that is used as a basis of analysis; (3) Analysis and extraction of outputs what are able to characterize the effects of different safety barrier strategies.

III. METHODOLOGY

A *bow-tie model* depicts the relationships between hazardous events, their causes, consequences, and associated barriers [42]. The bow-tie model places the hazards event in the center, the causes to the left, and the consequences to the right. A separate bow-tie diagram is established for each hazardous event. A hazardous event in a traditional risk analysis relates to events that may, if not responded to, may develop into major accidents. Examples from process industry include gas leakages and pressures above design limits. In this paper, a hazardous event is referred to a single failure.

A system is seldom subject to only one hazardous event, but several. The same assumption applies to cascading failures and CCFs. It is therefore necessary to model more than one bow-tie diagrams to capture dependences between the failures. Examples of such interactions are shown in Fig.1.

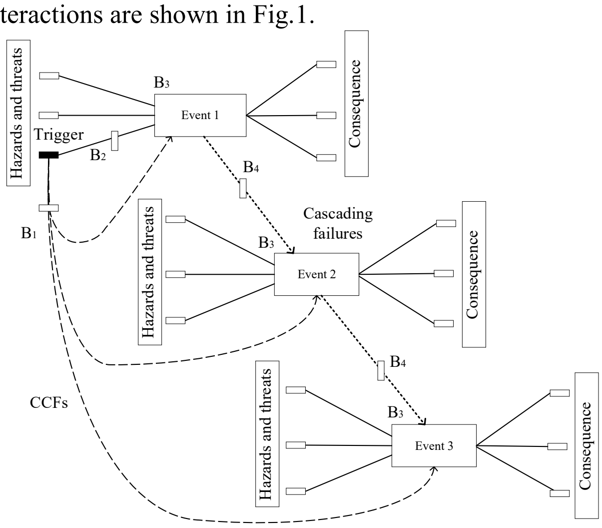

Fig.1 Extended bow-tie models

Traditional risk analysis defines often the first departure from normal operation as a *trigger event*. For example, [41] defines a triggering event as "an event or condition that is required for a hazard to give rise to an accident". Translated into the context of CCFs and cascading failures, we may consider the triggering events as root causes.

Safety barriers are used as the measures to prevent or mitigate the consequences of failures. We adopt this concept when introducing preventive and mitigating measures for CCFs and cascading failures. In our extended model in Fig. 1, we have introduce four safety barriers B_i (i=1, 2, 3, 4) for illustration, which is elaborated in the following subsections. To model effects of CCFs and cascading failures, we may consider failures and safety barriers in the extended bow-tie diagram.

A. Failures in the Extended Bow-tie Model

It is noted that we identify CCFs and cascading failures differently in the extended bow-tie model. If the failures arise from a common trigger event (i.e. common cause for more than one bow-tie diagram), we regard them as CCFs. For example, in Fig. 1, a shared cause triggers the failure of event 1, event 2 and event 3 at the same time. Such failures are CCFs. If one trigger event lead to the first failure and then results in the occurrence of other failures, the failures are cascading failures. For example, when the occurrence of event 1 lead to event 2, and event 3, such chain events are cascading failures.

CCFs are "first in line" failures [7], which implies that events and root causes are directly connected, and the multiple events may be simultaneous. Meanwhile, the occurrences of cascading failures are based on a series of interactions, conditioned with single preceding component failures. In other words, CCFs highlight direct cause-effect relationship, whereas cascading failures involve the interactions or dependencies between the components.

B. Barriers in the Extended Bow-tie Model

We may adopt different safety barrier strategies to prevent or mitigate the effects of cascading failures or CCFs. In general, there are four types of safety barriers in the extended Bow-tie model: B_1, B_2, B_3 and B_4, as illustrated in Fig. 1.

a. Barriers against effects of root causes

Many safety barriers are designed to prevent the failures that arise from the root causes. The function of the safety barriers against root causes of CCFs and root causes of cascading failures is the same. They are effective for both CCFs and cascading failures, while the locations are different:

1) B_1s against root causes of CCFs. Such safety barriers are to separate all the components from root causes so that they can protect all the components from the multiple failures simultaneously. For example, a cabinet may be introduced to protect equipment from exposures from radiation or fire.

2) B_2s against root causes of cascading failures. Those safety barriers aim to prevent initiation of the first failure. That may be spatial and temporal separations between the root cause and the first component to decrease the probability of the initiation of the failures.

b. Barriers against coupling effects

Several safety barriers aim to reduce the effects of failures regarding coupling factors and coupling paths:

1) B_3s against the effects from coupling factors of CCFs. Some safety barriers are to mitigate the effects of coupling factors. The efficient safety barriers for CCFs may be diversity of the components, different design and maintenance procedure.

2) B_4s against the effects from coupling paths of cascading failures. The safety barriers to intervene coupling paths of cascading failures can stop or slow down the failure propagation. Possible strategies of B_4s may include:

Strategy 1: Separation, e.g. physical separation on the coupling paths. Separation is to interrupt the connection between components [11]. Firewalls between facilities are typical measures to prevent the spread of fire on the coupling paths. Shutdown valves can isolate related process segments in case of some abnormal situation. They can stop or limit the medium flow, and thereby cease propagation of the failures.

Strategy 2: Removal, e.g. removing intermediate through the coupling paths. Removal of intermediates on the coupling paths is a measure to prevent failures propagation. Cascading failures often start with an initiating failure and develop into the second, the third and so on in the sequence. Removing some of the intermediates is to stop the propagation of the sequential failures. Such a strategy is widely adopted in power grid and internets.

Strategy 3: Improvement, e.g. improving absorptive ability or resistant capacity of the components. Improvement of absorptive or resistant capacity is to build in resistance of the components to tolerate the deviation [11, 20]. It can reduce the probability of overload that the first failure shifts its load to others. Examples of improvement strategies include mitigations on the highest load component, and enhancing capacity of the most connected components.

We present some specific examples of safety barriers in Table 1. In sum, safety barriers against CCFs emphasize on preventing and controlling coupling factors simultaneously, while the safety barriers against cascading failures are to stop or slow the propagation through coupling paths. The extended bow-tie model is an efficient tool to identify difference between CCFs and cascading failures, and corresponding safety barriers.

TABLE I

EXAMPLES OF SAFETY BARRIERS

Failure	Effect	Description	Barriers	Cat.
FTO [a] PSVs [b]	Root causes effects	The heating cable in the pilot line is disconnected due to short circuit	Implement regular quality check of heating cable	B_1
	Couplin g effects	Same design from one supplier	Replacing the existing cables with the ones from another company	B_3
Fire	Root causes effects	The cable is overheat due to short circuit, which lead to the fire and explosion	Redesign and regular check	B_2
	Couplin g effects	Fire and explosion propagating	Firewall to prevent fire explosion	B_4

[a] FTO: fail to open; [b] PSV: pressure safety valves;

V. RESULTS

The effects of different safety barrier strategies to defend against dependent failures may be studied using reliability analysis. To illustrate our suggested modeling approach, we have introduced a system comprising five components in a mixed (series and parallel) RBD structure. CCFs and cascading failures are illustrated in Figs. 2(a) and 2(b). Monte Carlo simulation was used to compute the system reliability. The coupling factors and coupling paths are the real factors to separate dependent failures from the other failures. Hence, in this case, we focus on safety barriers against coupling effects, namely B_3s for CCFs, and B_4s for cascading failures.

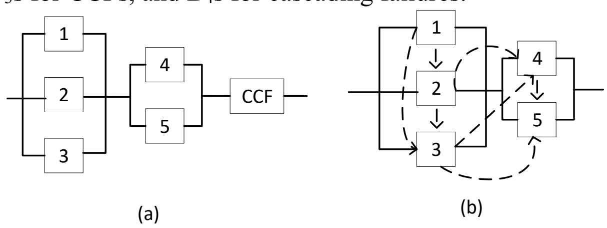

Fig. 2. System structures with CCFs and cascading failures

A. Assumptions

The assumptions for analyzing the effects of the safety barriers based on the extended bow-tie models are listed as follows:

1) All components are identical and unrepairable. Only two states are concerned: perfectly functioning and completely failed

2) Each component may be subject to both dependent and independent failures. Independent failures follow the exponential distribution with a constant failure rate λ.

In addition, the analysis for CCFs is based on the β-factor model introduced by Fleming [29]. All components may be subject CCFs at the same time. Total failure rates of one component can be written as the sum of the failure rates for independent failures and common cause failures:

$$\lambda = \lambda^{(i)} + \lambda^{(c)} \tag{1}$$

$\lambda^{(i)}$ denotes the failure rate due to independent failures, while $\lambda^{(c)}$ denotes the failure rate due to CCFs. The factor β is a conditional probability to express a failure of a channel is a common-cause failure:

$$\beta = \lambda^{(c)} / (\lambda^{(i)} + \lambda^{(c)}) \tag{2}$$

The safety barriers B_3s are introduce to reduce the effects of coupling factors on all components, where β can decrease.

When modeling of cascading failures, the conditional failure probability is a measure of dependency. This is a transition of failures taking place for the component *j* as soon as component *i* fails. The probability is defined as:

$$p = p_r(Comp.\, j\ fails | comp.\, i\ fails) \tag{3}$$

This conditional probability can be estimated from test data or historic failure data by either parametric or nonparametric techniques. Given a structure with n component, we arrange conditional probability as a matrix $\boldsymbol{P}$ that represents coupling paths among n components.

We consider three safety barrier B_4s as explained in the previous section: 1) Strategy 1, adopting a separation barrier between component 1 and component 2. 2) Strategy 2, removing a propagation intermediate component 2. 3) Strategy 3, improving absorptive load ability for all the components.

B. Case study

For simplicity, β in the CCF model is assigned as 0.3 for all components and p in the cascading model is assumed as fixed values 0.3 at first. The independent failure rate is 0.001 per hour. We used 10^5 Monte Carlo iterations over a period of 10^4 hours.

When introducing different measures B_3s against the effects of CCFs, β can decrease from 0.3 to 0.2, 0.1 and 0. The system reliabilities over time are illustrated in Fig. 3 (Time=2 Months). The blue curve reflects reliability of the system without any safety barrier. The red, yellow and purple curves refer to reliability of the systems with different safety barriers. It is obvious that the system reliabilities increase with a decrease of beta factors β. The beta factors represent the effectiveness of safety barriers B_3s by reducing the effects of coupling factors.

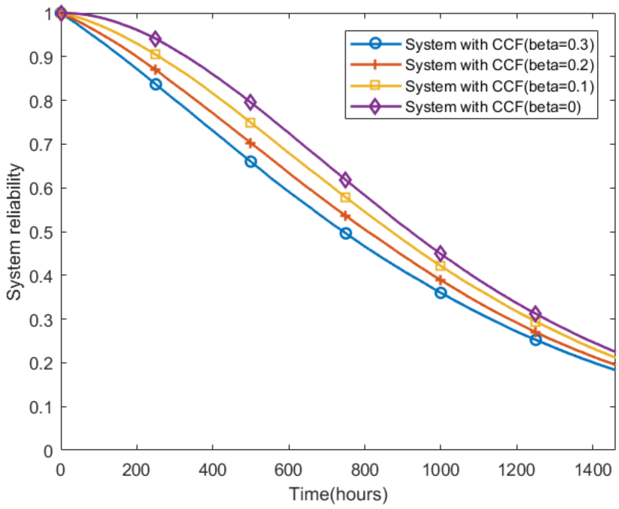

Fig. 3 The effects of safety barrier B2s for CCFs

Fig. 4 illustrates the effects of safety barriers B_4s on controlling cascading failures under the three different strategies. The strategy 1 decreases the conditional probability p from 0.3 to zero between component 1 and component 2. The strategy 2 removes component 2, which changes of conditional probability matrix $\boldsymbol{P}$. By increasing capacity of all the components in the strategy 3, the conditional probability p drops from 0.3 to zero.

In this case, the strategy 3 leads to the highest reliability. The effects of these safety barriers on the system reliability can reflect the decrease of conditional probabilities p of all the components. We cannot arbitrarily get a conclusion that the strategy 3 is always more effective. The observation results demonstrate that the effectiveness of barrier strategies are not same. It is necessary to consider the difference when designing barriers against dependent failures.

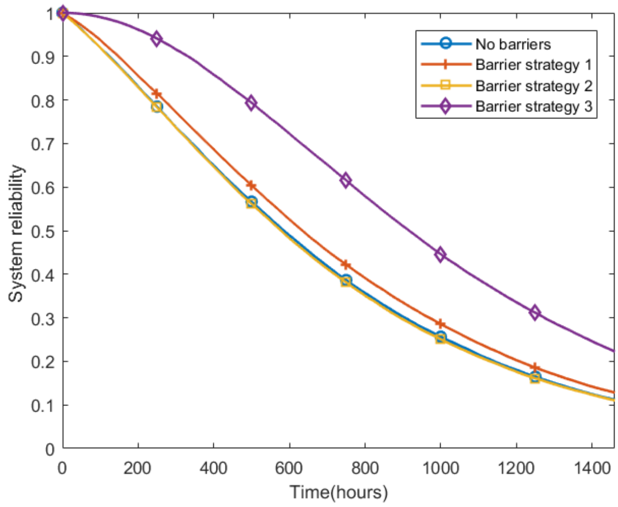

Fig. 4. The effects of safety barrier B4s for cascading failures

VI. CONCLUSION

It is important to consider efficient barrier strategies on reducing and mitigating effects of dependent failures in technical systems. The development of these strategies needs further explorations.

Our further work will involve the analysis of the importance and locations of safety barriers, for better protecting complex systems against dependent failures. More researches on safety barrier optimization are also required. In addition, more system structures, such as network systems, will be involved in the analysis.

REFERENCES

[1] K. Tsilipanos, I. Neokosmidis, D. Varoutas, "A system of systems framework for the reliability assessment of telecommunications networks," *IEEE Systems Journal,* vol.7, no. 1, pp.114-124, 2013.

[2] F.I. Khan, S. Abbasi, "Models for domino effect analysis in chemical process industries," *Process Safety Progress,* vol.17, no. 2, pp.107-123, 1998.

[3] M. Rausand, A. Høyland, *Book System reliability theory: models, statistical methods, and applications*, Hoboken, New Jersey, USA: *John Wiley & Sons*, 2004, pp.209.

[4] V. Cozzani, G. Spadoni, G. Reniers, "Approaches to Domino Effect Prevention and Mitigation", in *Domino Effects in the Process Industries*,Amsterdam: *Elsevier*, 2013, ch. 8, pp.176-188.

[5] N. Khakzad, F. Khan, P. Amyotte, V. Cozzani, "Domino effect analysis using Bayesian networks," *Risk Analysis,* vol.33, no. 2, pp.292-306, 2013.

[6] S. Sklet, "Safety barriers: Definition, classification, and performance," *Journal of loss prevention in the process industries,* vol.19, no. 5, pp.494-506, 2006.

[7] A.M. Smith, I.A. Watson, "Common cause failures—a dilemma in perspective," *Reliability Engineering,* vol.1, no. 2, pp.127-142, 1980.

[8] P. Humphreys, A.M. Jenkins, "Dependent failures developments," *Reliability Engineering & System Safety,* vol.34, no. 3, pp.417-427, 1991.

[9] H.M. Paula, D.J. Campbell, D.M. Rasmuson, "Qualitative cause-defense matrices: Engineering tools to support the

analysis and prevention of common cause failures," *Reliability Engineering & System Safety,* vol.34, no. 3, pp.389-415, 1991.

[10] M.A. Lundteigen, M. Rausand, "Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing," *Journal of Loss Prevention in the process industries,* vol.20, no. 3, pp.218-229, 2007.

[11] J. Janssens, L. Talarico, G. Reniers, K. Sörensen, "A decision model to allocate protective safety barriers and mitigate domino effects," *Reliability Engineering & System Safety,* vol.143, no. pp.44-52, 2015.

[12] J. Wang, "Mitigation strategies on scale-free networks against cascading failures," *Physica A: Statistical Mechanics and its Applications,* vol.392, no. 9, pp.2257-2264, 2013.

[13] A.E. Motter, "Cascade control and defense in complex networks," *Physical Review Letters,* vol.93, no. 9, pp.098701, 2004.

[14] J. Ash, D. Newth, "Optimizing complex networks for resilience against cascading failure," *Physica A: Statistical Mechanics and its Applications,* vol.380, no. pp.673-683, 2007.

[15] K. Peters, L. Buzna, D. Helbing, "Modelling of cascading effects and efficient response to disaster spreading in complex networks," *International Journal of Critical Infrastructures,* vol.4, no. 1-2, pp.46-62, 2008.

[16] IEC60050, "International Electrotechnical Vocabulary," Geneva, *International Electrotechnical Commission,* 1990.

[17] M. Rausand, *Book Reliability of safety-critical systems: theory and applications*, Hoboken, New Jersey, USA: *John Wiley & Sons*, 2014,

[18] SRDR418, "Dependent failures procedures guide," *United Kingdom Atomic Energy Authority, Safety and Reliability Directorate,* 1989.

[19] IEC61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems," Geneva, *International Electrotechnical Commission,* 2010.

[20] M. Ouyang, "Review on modeling and simulation of interdependent critical infrastructure systems," *Reliability engineering & System safety,* vol.121, no. pp.43-60, 2014.

[21] L. Xing, A. Shrestha, Y. Dai, "Exact combinatorial reliability analysis of dynamic systems with sequence-dependent failures," *Reliability Engineering & System Safety,* vol.96, no. 10, pp.1375-1385, 2011.

[22] J.G. Torres-Toledano, L.E. Sucar, "Bayesian networks for reliability analysis of complex systems," in *Ibero-American Conference on Artificial Intelligence*, IBERAMIA, pp. 195-206.

[23] Y. Chen, L. Yang, C. Ye, R. Kang, "Failure mechanism dependence and reliability evaluation of non-repairable system," *Reliability Engineering & System Safety,* vol.138, no. pp.273-283, 2015.

[24] S.M. Iyer, M.K. Nakayama, A.V. Gerbessiotis, "A Markovian dependability model with cascading failures," *IEEE Transactions on Computers,* vol.58, no. 9, pp.1238-1249, 2009.

[25] NEA, International common-cause failure data exchange. ICDE general coding guidelines. . 2004, Organisation for Economic Co-Operation and Development-Nuclear Energy Agency: Paris.

[26] G.W. Parry, "Common cause failure analysis: a critique and some suggestions," *Reliability Engineering & System Safety,* vol.34, no. 3, pp.309-326, 1991.

[27] NUREG/CR-4780, "Procedures for treating common cause failures in safety and reliability studies," Washington, DC, *U.S. Nuclear Regulatory Commission,* 1989.

[28] B. Harris, "Stochastic models for common failures," *Reliability and Quality Control,* no. pp.185-200, 1986.

[29] K. Fleming, "Reliability model for common mode failures in redundant safety systems", in *Modeling and simulation*, 1975, ch. 1,

[30] W. Vesely, "Estimating common cause failure probabilities in reliability and risk analysis: Marshall-Olkin specializations," *Nuclear systems reliability engineering and risk assessment,* vol.2, no. 314-341, 1977.

[31] S. Hauge, A. Hoem, P. Hokstad, S. Habrekke, M.A. Lundteigen, Common Cause Failures in Safety Instrumented Systems. 2015, SINTEF: Trondheim, Norway.17.

[32] V. Cozzani, G. Gubinelli, G. Antonioni, G. Spadoni, S. Zanelli, "The assessment of risk caused by domino effect in quantitative area risk analysis," *Journal of hazardous Materials,* vol.127, no. 1-3, pp.14-30, 2005.

[33] D. Murthy, D. Nguyen, "Study of a multi-component system with failure interaction," *European Journal of Operational Research,* vol.21, no. 3, pp.330-338, 1985.

[34] D. Murthy, D. Nguyen, "Study of two-component system with failure interaction," *Naval Research Logistics (NRL),* vol.32, no. 2, pp.239-247, 1985.

[35] A.E. Motter, Y.-C. Lai, "Cascade-based attacks on complex networks," *Physical Review,* vol.66, no. 6, pp.065102, 2002.

[36] R. Albert, A.-L. Barabási, "Statistical mechanics of complex networks," *Reviews of modern physics,* vol.74, no. 1, pp.47-97, 2002.

[37] B. Liu, J. Wu, M. Xie, "Cost analysis for multi-component system with failure interaction under renewing free-replacement warranty," *European Journal of Operational Research,* vol.243, no. 3, pp.874-882, 2015.

[38] V. Cortellessa, V. Grassi, "A modeling approach to analyze the impact of error propagation on reliability of component-based systems," in *International Symposium on Component-Based Software Engineering*, A modeling approach to analyze the impact of error propagation on reliability of component-based systems, Berlin, Heidelberg, pp. 140-156.

[39] M. Rausand, *Book Risk assessment: theory, methods, and applications*, Hoboken, New Jersey, USA: *John Wiley & Sons*, 2013, pp.2.

[40] PSA, Principles for barrier management in the petroleum industry. 2013, Petroleum Safety Authority Norway.

[41] M. Rausand, *Book Risk assessment: theory, methods, and applications*, Hoboken, New Jersey, USA: *John Wiley & Sons*, 2013, pp.364.

[42] J. Cockshott, "Probability bow-ties: a transparent risk management tool," *Process Safety and Environmental Protection,* vol.83, no. 4, pp.307-316, 2005.