Safety and Reliability – Safe Societies in a Changing World – Haugen et al. (Eds)
© 2018 Taylor & Francis Group, London, ISBN 978-0-8153-8682-7

Common cause failures and cascading failures in technical systems: Similarities, differences and barriers

L. Xie, M.A. Lundteigen & Y.L. Liu
NTNU, Trondheim, Norway

ABSTRACT: Many technical systems continue to increase in size and complexity, with more interactions and interdependencies between components. Dependent failures, such as common cause failures and cascading failures, are becoming important concerns to system reliability. Both failure types may lead to the unavailability of multiple components at the same time or within a short time interval. Although many researchers have studied common cause failures and cascading failures respectively, there is little comparison of the two concepts. This paper investigates the similarities and differences of these two failure groups, with focus on the conditions and nature of initiations and propagation of such failures. Moreover, a comparison is also made about suitable barrier strategies that can either prevent or reduce the consequences of failure. The paper concludes the study with a demonstration of reliability modeling for common cause- and cascading failures.

1 INTRODUCTION

Technical systems, such like railway systems, processing systems in chemical and petroleum plants, and power grids, are becoming increasingly complex. These systems include many physical components, with a huge number of interaction and interdependencies. Sometimes, those failures occurring in multiple components are resulted from the interconnections. We refer to such failures as dependent failures. Within the category of dependent failures, there are two sub-categories that are of specific interest: common cause failures (CCFs) and cascading failures (Rausand and Lundteigen, 2014). In the chemical and process industry, cascading processes are called as domino effects (Abdolhamidzadeh et al., 2010, Abdolhamidzadeh et al., 2009, Landucci et al., 2016).

Past accidents and near misses have shown that dependent failures are one of main threats to a complex system. For example, CCFs are main contributors of failures in safety systems of the oil and gas industry (Smith and Simpson, 2004, Lundteigen and Rausand, 2007). Fires in the chemical and process industry highlight the severe cascading consequences (Landucci et al., 2016, Cozzani and Reniers, 2013). The blackouts in United States, Canada in 2003, and Europe in 2006 are also the examples of cascading failures (Kotzanikolaou et al., 2013, Andersson et al., 2005). Many other infrastructure systems, like water distribution networks, transportation, also often suffer from cascading failures (Lin et al., 2014, Shuang et al., 2014, Ouyang, 2014).

So far, it seems like most attention has directed to CCFs and in specific for safety-critical systems where redundancy is used actively to enhance reliability (Paula et al., 1991, Humphreys and Jenkins, 1991, Lundteigen and Rausand, 2007, IEC61508, 2010, A. Mosleh, 1998). There have been two main strategies suggested for incorporating defenses against CCFs in design. One is to carry out analyses to identify and remove causes, and the other is to introduce measures to reduce the effects of CCFs in case they occur. Suggested methods include cause-defense matrices, common cause analysis, and zonal analysis (Humphreys and Jenkins, 1991, Paula et al., 1991).

The defenses to CCFs are typically identified in design, however, measures in the operational phase are also important (Lundteigen and Rausand, 2007). Even for an excellent system design, there will always remain a risk of CCFs. It is therefore required to include the contribution of CCFs in quantitative analyses used to demonstrate adequate reliability. A high number of models has been introduced for this purpose (Vesely, 1977, Fleming, 1975, Evans et al., 1984, Mosleh and Siu, 1987). The standard beta factor model is perhaps the most widely adopted, due to its simplicity (Fleming, 1975, IEC61508, 2010). The PDS method (Hauge et al., 2015) is an extension of the standard beta factor, where a second parameter is added to account for voting, e.g. 2-out-of-3 and 1-out-of-3.

As for cascading failures, it is of interest to consider efficient means to avoid or reduce the vulnerability of the failures in the system design, and to quantify cascading failures. An important

task in these analyses is to study interdependencies, and many analyzing approaches in literature are based the topology of complex network (Motter and Lai, 2002, Wang, 2012, Albert and Barabási, 2002). One kind of cascading failures are the failures when a heavily load component fails, and its load is redistributed to other components, resulting in loads on that exceed their capacities. State-based approaches, such as Markovian process, approaches based on the Bayesian network models, and Monte Carlo Simulation have been used to analyze cascading failures (Iyer et al., 2009, Calviño et al., 2016, Erp et al., 2017).

In fact, many technical systems can be subject to both CCFs and cascading failures, thus it is important to consider both failure categories in reliability analysis. Unfortunately, very limited attention has been directed comparing the two types of dependent failures, and their corresponding defense strategies. Kotzanikolaou et al. (2013) highlight that CCFs may have cascading effects, but do not go into much detail.

The objective of this paper is therefore to make a comprehensive comparison on the concepts, causes, and mechanisms of the two failures, and provide some suggestions on the analysis and defense strategies. In this paper, we use the term of barrier to denote a specific defense measure.

The rest of the paper is organized as follows: In section 2, we discuss the definitions and interpretations of CCFs and cascading failures. Sections 3 and 4 present the similarities and distinctions of the two failures. In section 5, we clarify the barriers against the two failures. A small example is then employed in section 6, to illustrate that the effects of CCFs and cascading failures. Conclusions and discussions occur in section 7.

2 DEFINITIONS AND INTERPRETATIONS

According to Humphreys and Jenkins (Humphreys and Jenkins, 1991), *dependent failures refer to the failures whose probability cannot be expressed by unconditional probability of the individual event*. Dependencies in a technical system may derive from the sameness of the types of components, exposure from the same environment, the use of shared resources, functionality, the common shocks and the incapability to resist certain hazardous events (Rausand, 2013).

People in different industrial sectors define CCFs in their own ways. Nuclear sector defines it as *two or more component fault states exist at the same time, or with a short interval, because of a shared cause* (Mosleh et al., 1988). The generic standard on design and operation of electric, electronic, and programmable electronic safety-related systems, IEC 61508, 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 a multiple channel system, leading to system failure* (IEC61508, 2010). Both definitions emphasize that CCFs involve at least two failures that are due to a shared or common cause.

Cascading failure may be *multiple failures, where initiated by the failure of one component in the system that results in a chain reaction, the so-called domino effect* (Rausand and Øien, 1996). In power systems, cascading failure is referred to *a sequence of dependent failures of individual components that successively weakens the systems* (Baldick et al., 2008). It differs from the definition in infrastructures that limit the cascading failure to the propagation of failures between components (Rinaldi et al., 2001). Generally, we can find some same elements in the definitions that cascading failures are multiple failures initiated by one, and a sequential effect occurs.

From the perspective of failure causes, both CCFs and cascading failures result from some common vulnerabilities of more than one component. These two types of failures are interrelated in some cases (Laprie et al., 2007, Kotzanikolaou et al., 2013). However, they are still two distinctive categories of dependent failures. As Smith and Watson explained, CCFs emphasize that failures are located in 'first in line', which means that the failure are only dependent on the causes, but not on each.

In the following sections, we try to elaborate similarities and difference between the two failures.

3 SIMILARITIES

We categorize the similarities between CCFs and cascading failures into three: *multiplicity*, *timeliness* and *classification of causes*.

3.1 *Multiplicity*

Both CCFs and cascading failures obviously involve more than one components. We are concerned with the *effect of failure* of several components and *functions* for two categories of failures.

3.2 *Timeliness*

For both CCFs and cascading failures, the time from the first failure to the existence of multiple failures is often short. In case of insufficient mitigation measures, the collapse of an entire system may occur very soon. For example, in the Three Mile Island accident caused by CCFs in 1979, the radiation level in the primary coolant water

was around 300 times of the expected level after only 2 hours (Hasani, 2017). The power blackout in India in 2012 due to cascading failures, spread across 22 states within 12 hours and affected more than 620 million people (Russel, 2012).

3.3 *Root causes*

Root causes of both CCFs and cascading failures are the common vulnerability of more than one components in a system. Coupling factors between components can explain why multiple components are destroyed by a common hazardous event, e.g. cold temperature, extreme snowfall or electrical failure. Meanwhile, for cascading failures, couplings also can explain why multiple components are affected by the faults of relevant components. For example, the unavailability of one processing unit increases the workload of another unit.

4 DIFFERENCES

For differences between two types of failures, we categorize them into two: *initiation* and *propagation* of failures, as shown in Table 1. Initiation of failures.

As seen in Table 1, the initiating event of a CCF can be either replicated or occur simultaneously for several components. The effect of CCFs arises from shared causes, may be simultaneous failures or failures with some time apart. A cascading failure always starts with a single preceding component failure, as the effect of an initiating event.

Table 1. Differences between CCFs and cascading failures.

Difference	Characteristics	CCFs	Cascading failures
Initiation	Triggering condition	Shared causes	Conditional on preceding failures
	Occurrence	Simultaneously or during a critical time of interest	Sequence
Propagation	Sequence	First in line	Series
	Consequence	Finite	Possibly infinite
	Pathway	Cause-components	Connected/ dependent components

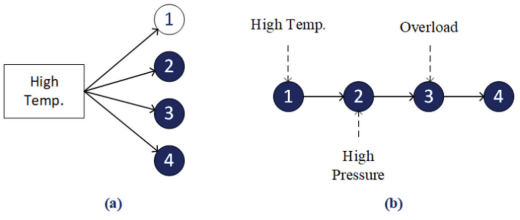

Figure 1. CCF and cascading failures.

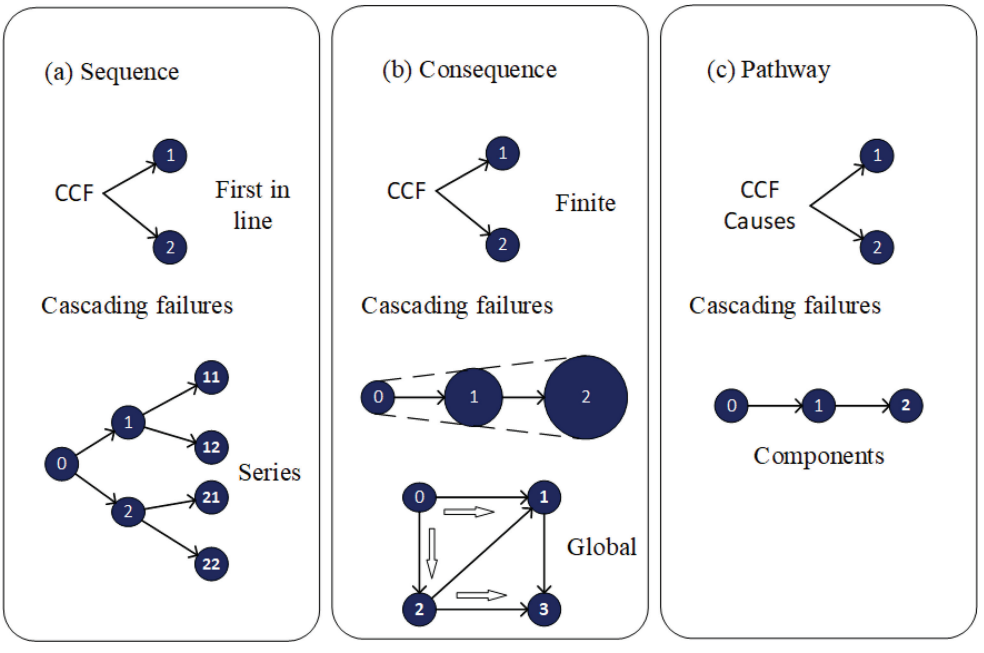

Figure 2. Comparisons of CCFs and cascading failures in terms of impact and effect.

To illustrate these differences, we introduce two small examples, as shown in Figure 1. High temperature is the initiating event of both a CCF and a cascading failure in this case. In Figure 1(a), all the four components expose themselves to high temperature, and so all or some of the components fail simultaneously or in a short interval. However, in the case of a cascading failure of Figure 1(b), only component 1 is exposed to high temperature, and fails due to this initiating event. Then, the failure of component 1 trigger the failures of other components due to diverse reasons. Even in the same cascading sequence, the failure causes can be different for the different components.

4.1 *Propagation of failures*

Propagation of failure means in this context the evolvement of multiple failures, with the initiating event already manifested. Figure 2 illustrates the differences in the propagation of CCFs and cascading failures. CCFs are *first in line* failures that delineate the exclusion of dependent failures from CCF definition (Smith and Watson, 1980), which implies that CCFs are directly linked to the failure causes. On the contrary, the propagation of a cascading failure follows a series of interactions. CCFs are most different from cascading failures in terms of the approaches of propagation. As shown in Figure 2(a), for CCFs, the first in line failure only occurs on component 1 and 2. For the consequence of failure propagation, as shown in Figure 2(b), a cascading failure can escalate and result in worse impacts on the other parts of a system, such as more serious disruptions, overload to neighbors and longer recovery time etc. CCFs highlight a direct cause-effect relationship between the cause and the failed components (Rausand and Lundteigen, 2014), whereas the pathway of cascading failures involve the interactions or dependencies between relevant components, see in Figure 2(c).

5 BARRIERS

Barriers are employed to prevent, control or mitigate undesired events or accident (Sklet, 2006). Sometimes, barriers are also called defenses, protection layers or countermeasures. In general, a barrier function can be realized by many different means, such as by a technical or physical system, human actions and procedural deficiencies.

In the design phase of a system, it is possible to introduce barriers against potential failures, like separation, diversity, quality control, simplicity of design etc. Some of them are effective to reduce the probability of CCFs, and some of them are more functional for protecting the system from cascading failures. Considering the similarities and differences of CCFs and cascading failures, we can categorize barriers into three groups: *barriers against both failures*, *barriers against CCFs* and *barriers against cascading failures*.

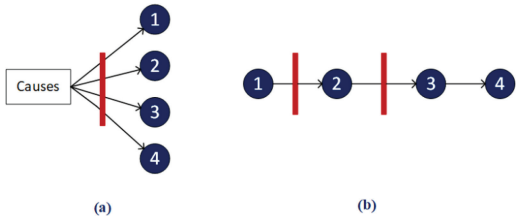

Figure 3. Barriers for CCF and cascading failures.

- Barriers efficient for both failures: Such kind of barriers should be designed in consideration of the similarities of CCFs and cascading failures, such like their root causes and coupling factors. One way of barrier design is therefore to mitigate and reduce the vulnerability to root causes. Simplicity can be regarded as a barrier, for example, to reduce system complexity that is one important source of vulnerability. Another way of barrier design is to decrease the coupling degrees among components. Spatial and temporal separations are examples of decreasing coupling degrees. In practices, we can find that firewalls in a process plant are effective barriers to prevent fire disasters.
- Barriers against CCFs: The effectiveness of such barriers is to isolate failure causes and components, as shown in Figure 3(a). One example is diversity of the design. Diverse components will often have different failure modes, and are therefore less likely to be affected by the common cause. However, diversity is not effective to mitigate cascading failures. When the failure of one component brings higher workload to its neighbors and their failure probabilities, no matter the components are identical or not.
- Barriers against cascading failures: The main purposes of this kind of barriers are to stop or slow down failure propagation, as shown in Figure 3(b). An example for this class of barriers is a process shutdown valve that can isolate related process segments. In case abnormal events have occurred in the upstream facility, the shutdown valve can stop or limit the flow between two facilities, and thereby cease the failure propagation.

In the next section, we will use a small example to illustrate the quantitative analyses for CCFs and cascading failures, and the effects of barriers.

6 CASE STUDY

Suppose a system comprising two parallel components. The effects of failures and corresponding barriers for the two dependent failures are studied separately, as illustrated in Figure 4.

For modeling CCFs, a new *independent* "CCF" event is added in the standard beta model with beta-factor β. The parameter β can be interpreted as the conditional probability that a failure of a channel is in fact a common-cause failure:

$$\beta = \Pr(CCF \,|\, Failure\ of\ channels) \tag{1}$$

With inclusion of CCFs, the total system reliability can be obtain as:

$$R(t) = 2R - R^{(2-\beta)} \tag{2}$$

where $R = 0.8$ and $\beta = 0.1$.

For modeling cascading failures, it is necessary to consider the effects of functional dependency between the two components, and Bayesian network model is an approach we used here. The conditional failure probability is a measure of dependency that differ from the conditional probability β for CCFs. The conditional probability for cascading failures can be defined as:

$$\Pr(Comp.B\ fails \,|\, comp.A\ fails) = \frac{F_D}{F_A} \tag{3}$$

Here, F_A and F_B denote the individual failure probability for component A and B. F_D denotes the failure probability for component A on the condition of component A has failed. The total system reliability with cascading failures can be obtained as:

$$\begin{aligned} R(t) &= 1 - F_A(F_B + F_D - F_B F_D) \\ &= 1 - (1-R)^2 - (1-R)^2 RP_r \end{aligned} \tag{4}$$

where P_r denotes conditional probability between component A and B and is assigned as 0.1(Pr = 0.1).

As shown in Figure 5, the total system reliability with CCFs becomes 0.946, but it is 0.957 with the effects of cascading failures at that time. This

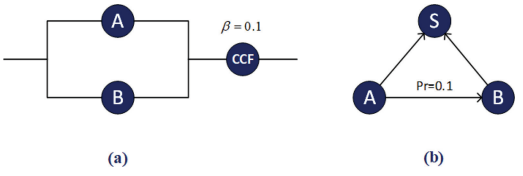

Figure 4. Case study for CCF and cascading failures.

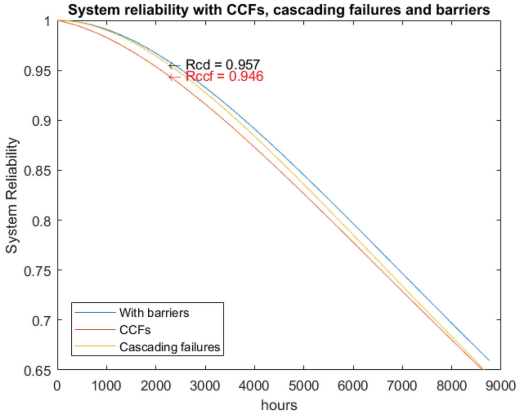

Figure 5. Reliability with cascading failures & CCFs.

implies that CCFs may have more influence on the reliability performance than cascading failures in this case, when using similar assumptions about the probability of having additional failures, when a first failure has occurred.

We now introduce time-dependent probabilities for reliability analysis, and assume that the time to failure is exponentially distributed, with failure rate of 1E-04 per hour for each component. For the system with CCFs, the total system reliability can be obtain as:

$$R(t) = \left[2e^{-(1-\beta)\lambda t} - e^{-2(1-\beta)\lambda t}\right] e^{-\beta\lambda t} \tag{5}$$

For the system with cascading failures, the total system reliability can be obtain as:

$$R(t) = 1 - (1 - e^{-\lambda t})^2 - (1 - e^{-\lambda t})^2 e^{-\lambda t} P_r \tag{6}$$

Figure 5 illustrates calculated system reliability considering the effects of the two failures as a function of time. We can see that, in this case, the two failures seems to have comparable effects on the system reliability.

For CCFs, the function of barriers is to separate shared root causes from the components. The function of the barriers against cascading failures is to prevent propagation of the failures between component A and B. Reliability of the system with barriers is illustrated in the blue line in Figure 5, implying that the system reliability will increase when performing barriers function against the failures.

7 CONCLUSION AND FURTHER WORK

Exploring similarities and difference between CCFs and cascading failures facilitate us to answer

the following questions: 1) why such dependent failures initiate, 2) how dependent failures contribute to disruptions in the systems, and 3) what kind of barriers are needed and how they should be implemented. In this paper, we find that CCFs and cascading failures may have comparable influences on the performance of a simple system. More probabilistic and quantitative analyses are required, to evaluate the impacts of cascading failures in a larger and more complex system (Erp et al., 2017).

Our further work will involve modeling the interdependent systems with cascading failures and CCFs, and developing tools to evaluate reliability for complex systems. It is also of interest to identify different failure modes and perform barrier analysis for both of the failures, which can help to allocate barriers and thereby optimize barrier functions.

REFERENCES

Abdolhamidzadeh, B., Abbasi, T., Rashtchian, D. & Abbasi, S.A. (2010) A new method for assessing domino effect in chemical process industry. *Journal of hazardous materials,* 182, 416–426.

Abdolhamidzadeh, B., Rashtchian, D. & Ashuri, E. (2009) A new methodology for frequency estimation of second or higher level domino accidents in chemical and petrochemical plants using monte carlo simulation. *Iranian Journal of Chemistry and Chemical Engineering (IJCCE),* 28, 21–28.

Albert, R. & Barabási, A.-L. (2002) Statistical mechanics of complex networks. *Reviews of modern physics,* 74, 47.

Andersson, G., Donalek, P., Farmer, R., Hatziargyriou, N., Kamwa, I., Kundur, P., Martins, N., Paserba, J., Pourbeik, P. & Sanchez-Gasca, J. (2005) Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance. *IEEE Transactions on Power Systems,* 20, 1922–1928.

Baldick, R., Chowdhury, B., Dobson, I., Dong, Z., Gou, B., Hawkins, D., Huang, H., Joung, M., Kirschen, D. & Li, F. (2008) Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures. *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE.* IEEE.

Calviño, A., Grande, Z., Sánchez-Cambronero, S., Gallego, I., Rivas, A. & Menéndez, J.M. (2016) A Markovian–Bayesian network for risk analysis of high speed and conventional railway lines integrating human errors. *Computer-Aided Civil and Infrastructure Engineering*, 31, 193–218.

Cozzani, V. & Reniers, G. (2013) Historical background and state of the art on domino effect assessment. *Domino Effects in the Process Industries: Modelling, Prevention and Managing.* Elsevier, Amsterdam, The Netherlands.

Erp, N.V., Linger, R., Khakzad, N. & Gelder, P.V. (2017) Report on risk analysis framework for collateral impacts of cascading effects. *RAIN—Risk Analysis of Infrastructure Networks in Response to Extreme Weather.* TU Delft.

Evans, M., Parry, G. & Wreathall, J. (1984) On the treatment of common-cause failures in system analysis. *Reliability engineering,* 9, 107–115.

Fleming, K. (1975) Reliability model for common mode failures in redundant safety systems. *Modeling and simulation. Volume 6, Part 1.*

Hasani, F. (2017) Calculation and Analysis of Reliability with Consideration of Common Cause Failures (CCF)(Case Study: The Input of the Dynamic Positioning System of a Submarine). *International Journal of Industrial Engineering & Production Research,* 28, 175–187.

Hauge, S., Hoem, A., Hokstad, P., Habrekke, S. & Lundteigen, M.A. (2015) Common Cause Failures in Safety Instrumented Systems. SINTEF Technology and Society Trondheim.

Humphreys, P. & Jenkins, A.M. (1991) Dependent failures developments. *Reliability Engineering & System Safety,* 34, 417–427.

Iec61508 (2010) Functional safety of electrical/electronic/programmable electronic safety related systems. *International Electrotechnical Commission*.

Iyer, S.M., Nakayama, M.K. & Gerbessiotis, A.V. (2009) A Markovian dependability model with cascading failures. *IEEE Transactions on Computers,* 58, 1238–1249.

Kotzanikolaou, P., Theoharidou, M. & Gritzalis, D. (2013) Cascading effects of common-cause failures in critical infrastructures. *International Conference on Critical Infrastructure Protection.* Springer.

Landucci, G., Argenti, F., Spadoni, G. & Cozzani, V. (2016) Domino effect frequency assessment: The role of safety barriers. *Journal of Loss Prevention in the Process Industries,* 44, 706–717.

Laprie, J.-C., Kanoun, K. & Kaâniche, M. (2007) Modelling interdependencies between the electricity and information infrastructures. *Computer Safety, Reliability, and Security*, 54–67.

Lin, Y., Li, D., Liu, C. & Kang, R. (2014) Framework design for reliability engineering of complex systems. *Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2014 IEEE 4th Annual International Conference on.* IEEE.

Lundteigen, M.A. & Rausand, M. (2007) 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,* 20, 218–229.

Mosleh, A., D.M. Rasmuson & F.M. Marshall (1998) Guidelines on modeling common cause failures in probablistic risk assessment.

Mosleh, A., Fleming, K., Parry, G., Paula, H., Worledge, D. & Rasmuson, D.M. (1988) Procedures for treating common cause failures in safety and reliability studies: Volume 1, Procedural framework and examples. Pickard, Lowe and Garrick, Inc., Newport Beach, CA (USA).

Mosleh, A. & Siu, N. (1987) A multi-parameter common cause failure model. *Transactions of the 9th international conference on structural mechanics in reactor technology. Vol. M.*

Motter, A.E. & Lai, Y.-C. (2002) Cascade-based attacks on complex networks. *Physical Review E,* 66, 065102.

Ouyang, M. (2014) Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability engineering & System safety,* 121, 43–60.

Paula, H.M., Campbell, D.J. & Rasmuson, D.M. (1991) Qualitative cause-defense matrices: Engineering tools to support the analysis and prevention of common cause failures. *Reliability Engineering & System Safety,* 34, 389–415.

Rausand, M. (2013) *Risk assessment: theory, methods, and applications*, John Wiley & Sons.

Rausand, M. & Lundteigen, M.A. (2014) *Reliability of safety-critical systems: theory and applications*, John Wiley & Sons.

Rausand, M. & Øien, K. (1996) The basic concepts of failure analysis. *Reliability Engineering & System Safety,* 53, 73–83.

Rinaldi, S.M., Peerenboom, J.P. & Kelly, T.K. (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems,* 21, 11–25.

Russel, H.S. a. R. (2012) 620 million withow power in india after 3 pewer grids fail.

Shuang, Q., Zhang, M. & Yuan, Y. (2014) Node vulnerability of water distribution networks under cascading failures. *Reliability Engineering & System Safety,* 124, 132–141.

Sklet, S. (2006) Safety barriers: Definition, classification, and performance. *Journal of loss prevention in the process industries,* 19, 494–506.

Smith, A.M. & Watson, I.A. (1980) Common cause failures—a dilemma in perspective. *Reliability Engineering,* 1, 127–142.

Smith, D.J. & Simpson, K.G. (2004) *Functional Safety: A straightforward guide to applying IEC 61508 and related standards*, Routledge.

Vesely, W. (1977) Estimating common cause failure probabilities in reliability and risk analysis: Marshall-Olkin specializations. *Nuclear systems reliability engineering and risk assessment,* 2.

Wang, J. (2012) Mitigation of cascading failures on complex networks. *Nonlinear Dynamics,* 70, 1959–1967.