Translation of Process Safety to Cyber Incidents within the Emergency Management Arc

Jennifer Schneider, Sarah Dobie and Salim Ghettas
Collaboratory for Resiliency and Recovery
Rochester Institute of Technology
Rochester, New York, USA

jlwcem@rit.edu, sdobie@umich.edu, sg6129@rit.edu

***Abstract*—Providing cybersecurity for critical infrastructure has become more challenging as the span and sophistication of cyber-physical risks continue to evolve. The potential impact of breaches, data loss, and operability concerns continue to increase across these complex, community-based technologically coupled systems. This paper finds that process safety management thinking can inform cyber-physical resilience efforts and ongoing cyber risk management, especially for critical infrastructure within the emergency management arc.**

Keywords— Situational awareness, community resilience, management systems, critical infrastructure, operational resilience, risk management.

I. INTRODUCTION

Cyber security issues, especially those in the cyber-physical risk arena are a growing concern. Technological systems, including critical infrastructure, are becoming more complex, making them more attractive and vulnerable to cyber-attacks. This can be extremely disruptive and costly to societies, especially as more information is stored in servers and smart technologies are integrated into these systems, creating additional points for infiltration. For example, a failure of electricity grids and the Information and Communication Technology (ICT) infrastructure cascades effects across various other sectors and even communities, posing a significant threat to national security if these systems lose data or operational control. Further, such losses can undermine recovery operations after a crisis, and therefore, cyber systems impacts are reflected in the physical and operational systems across the entire emergency management arc.

Cyber security is a unique challenge; however, there are opportunities to inform approaches from other human-physical-operational risk systems, such as industrial safety, and within that, process safety management (PSM). PSM techniques used in high hazard, complex applications for operational fitness and control of impact propagation can translate to these also complex cyber-physical system challenges we seek to address [1]. Further, cyber risk is inherent to overall process safety management, particularly in regards to engineering controls that rely upon SCADA (supervisory control and data acquisition) systems.

This paper adapts approaches from the PSM spectrum to include and inform cyber security. In section II, the paper introduces the evolution of generalized risk management, situational awareness and incident data taxonomies and their applicability to cyber security. Section III describes our methodology to derive the connections between PSM and cyber risk. Section IV discusses our initial results and future work, while section V concludes this paper by examining the applicability of PSM approaches to cyber-physical systems, from mitigation through response and recovery.

II. BACKGROUND

A. Historical development of risk management

Systematic risk management systems tend to mature in a common progression [2]. This evolution is generally triggered by an event that is ineffectively managed, triggering public reaction, which leads to laws and regulations, and eventually grows into a more proactive, mature management system approach. It is reasonable to assume that cyber security risk management will develop in a similar progression, as is indicated by its current state. Reaction to event failures, need for reliable operations, reputational impacts, etc. have pushed industrial risk management forward toward recognition of social responsibility, and driven a need to become more proactive and focused on prevention. While cyber risks are not completely analogous to process failures, we postulate that these same systemic drivers will continue to occur in cyber risk management over time. Integrating our risk knowledge and capabilities within a management system structure provides a powerful tool to manage and mitigate risks.

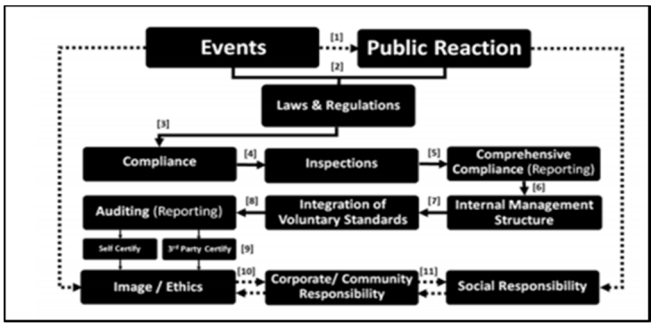

Fig. 1: Historical development of systemic risk management developed by Schneider et al. [2]

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

B. Role of event data in risk and emergency management

Development of a comprehensive risk management system requires a complete suite of emergency management approaches including hazard and risk identification, prevention, mitigation and incident response. While access to data and information is important along the entire emergency management arc, it is particularly critical in two phases, as a 'lessons learned' opportunity for mitigation of future vulnerabilities and as an ongoing source of situational awareness for responding to unfolding events. In both cases, event data informs decision-making. Situational awareness and sense-making in cyber risk management is different than traditional PSM event response. Typical cyber datasets have a high noise ratio, across the multiple data feeds of intrusion detection, firewall logs, information management systems, etc. Certainly, traditional PSM also employs data from multiple sources, but the event rate is much lower. For this reason, cyber operations centers rely heavily on humans to evaluate to data and to determine when to respond. When capture rates increase, analysts must determine if tools and methodologies are more effective or if malicious event rates are increasing, or both, through triage, escalation, threat, and incident response [3].

The methodologies for cyber risk sense-making are similar to traditional PSM and employ a loop format which follows an 'observe-orient-decide-act' (OODA) process, however the orient or data triage portion for cyber is rather complex [4]. The critical systems of critical infrastructure employ both software and data that are security related (data that is private) and safety related (operational). Fundamentally, *security* denotes that the process is unharmed, and *safety* denotes the process does not harm the world. This general orientation difference is notable for process safety versus cyber security. Further, it reflects the malicious actor mode (attacker/defender) that is part of cyber security. The DHS CFATS (Chemical Facility Anti-Terrorism Standards) regulation for chemical safety is notably process *security* oriented [5]. Regardless of the safety or security orientation, risks are not static, and therefore, assets (human, physical, operational) must be protected, threats and risks evaluated, and known vulnerabilities monitored. Despite privacy and reputational challenges, development and analysis of incident data both internally and as part of an external shared data repository allows experts to learn from collective experience and improve overall management. This is especially important as connectivity between cyber-physical systems of critical infrastructure increase, and new vulnerabilities arise. Others have shown that even attacker- defender incident analysis benefits from a severity level model, and that the attacker has the advantage even with hardening and increasing reliability by back up [3, 6, 7, 8]. Data can support assessment of controls, lessons learned from incidents, identification of trends and changes and emerging risks [3, 8].

C. Risk impact taxonomies

i. Heinrich's Safety Triangle

The gains in risk management in the process industries has resulted from the use of ever improving operational, human, and organizational information. As safety engineering matured in these environments, various system failure analysis tools were employed to further illuminate incident analysis. Decades ago, W. H. Heinrich described accident causation as a chain of conditions or events [9], which resulted in injury and developed a theory for accident occurrence that found that for every 300 near misses there are 29 major injuries and 1 serious injury or fatality (Figure 2). This hierarchy introduced the idea that there were occurrence ratios between incident severities, namely that lower severity incidents occurred more often than higher severity incidents, and if low severity occurrences were mitigated, higher severity were less likely to occur (or severity would decrease) [9]. We show injury examples here as a simple method to visualize the severity of impact, though this severity can be represented broadly across incident modalities.

While this theory has been of some debate [10,11], this type of thinking has evolved into a more systems driven and holistic view of risk management, becoming more proactive, predictive, and mitigative earlier in incident arcs, particularly in PSM applications in high hazard industries, expanding intervention and prevention actions and opportunities. The hierarchy does not illustrate a causal relationship between severity types, but rather illustrates the proportional relationship between impact severity types; for example, that low severity or near miss incidents are more likely to occur than high hazard incidents. Kupers, et al. noted in a similar cyber incident study that over time the rise in total incident occurrences was due to a rise in lower impact incidents, not major ones [6]. In fact, while there are instances where high impact incidents seem to be the 'first' occurrence in PSM, this is generally considered an indicator that management did not record lower impact incidents, or they were somehow hidden from view. The idea that all incidents, regardless of severity, are indicative of risk has been influential on the development of safety management systems. If cyber security has occurrence ratios, it may be useful for organizations to prevent cyber security impacts by managing root causes of near misses and lower impact incidents as a part of an overall risk management strategy. Further, typical incident management also continuously assesses the upper control limits for incident rates to determine if there is a process anomaly occurring that can be addressed.

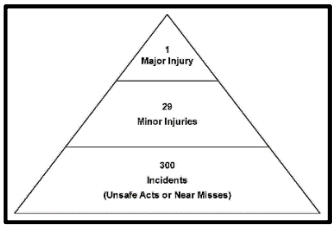

Fig. 2: Hierarchy of safety incidents developed by Heinrich [3]

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

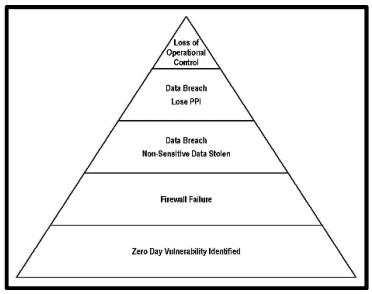

Fig. 3: Cyber security hierarchy for theft from an individual perspective

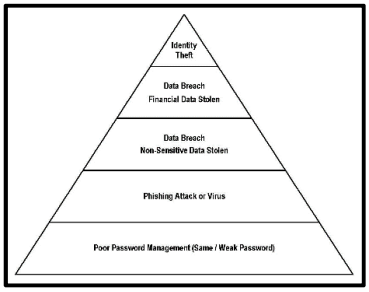

Fig. 4: Cyber security hierarchy for sabotage from a critical infrastructure (organizational) perspective

ii. Developing a Taxonomy for Cyber Security Risks

A taxonomy of operational cyber security risks was developed by Cebula and Young [7] merging taxonomies from the Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST), and CERT Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method. The taxonomy is broken into four categories of risks: actions of people, systems and technology failures, failed internal processes, and external events. Actions of people includes deliberate actions, such as fraud, sabotage, theft, and vandalism. Other authors divide by type into operational disruption, sensitive data loss, software vulnerabilities resulting from external threat, insider threat and mistake [6].While these taxonomies describes the different types of risks, and modes, neither set provides a hierarchical structure for understanding risk by impact severity. Heinrich's 'Safety Triangle' can be adapted for categorizing types of cyber security incidents. Figures 3 and 4 show examples of theft and sabotage, one from the perspective of an individual and another from the perspective of an organization. Note that the examples chosen are just a sample of what could be classified in this hierarchy.

III. METHODOLOGY

Since we are examining the usefulness of PSM approaches to cyber risk management, we begin by assessing the approaches of the major PSM standards for cyber incident focus. Due to the need for situational awareness both in PSM and cyber, we then examine an available case dataset to determine if generalized safety situational data hierarchical knowledge can be translated to cyber risk management. Given our preliminary assessment, we then suggest potential mitigation and management methods that can be refined for cyber incident risk management.

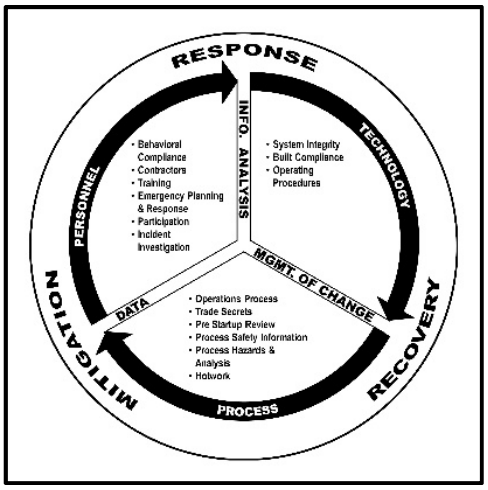

Fig. 5 Generalized PSM system

IV. RESULTS

A. Generalized PSM elements

There are several areas where PSM is especially applicable to cyber systems, and where cyber is also a critical component of PSM itself. See Figure 5 above.

i. *Hot work*, allowing work, under permit, that is inherently hazardous and completed by specially trained individuals, with interventions and controls available. Typically, in PSM, the work is actually 'hot', meaning that fire or chemical release could result. Such work requires management approval by documented permit for the specific case. In cyber systems, this is analogous to the system supervisor directly intervening while it is operational.

ii. *Contractors* are only allowed to interact with the process under controlled conditions, with approvals. Contractors must also be specifically trained for the conditions and actions they will encounter, and are responsible for maintaining system (and data) integrity, particularly because contractors can be brought in for specialized expertise or support functions. This need is aptly demonstrated in cyber driven systems.

iii. *Change Management* requires that any operational modification be documented and approved prior to implementation, important in any hazard propagation.

iv. *Information analysis* requires documentation of operational information to inform current and future performance. This is especially important after an incident, be it cyber or traditional PSM risks.

B. Comparison of PSM standards regarding cyber risk

Strikingly, while many experts acknowledge the need for control of cyber borne risk as part of PSM, a comparison of the major PSM standards shows that not all PSM management systems explicitly acknowledge cyber as an area of focus. See Table 1 [5, 12-21].

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

Table 1:COMPARISON OF PSM GUIDELINES AND REGULATIONS

PSM Guideline/Regulation/ Management System (publishing body)	Focus Area	Explicitly Includes Cyber Risk	Requires Incident-informed Management	Reporting Required to External Entity
Process Safety Management (OSHA 29CFR 1910.119 or EPA 40:68)	• Management of highly hazardous chemicals and process-related risks. • Prevention of process accidents. • Protection of workers, contractors, community, and public from process incidents and their impacts.	No	• Required to consider historical process events in Process Hazard Analysis (PHA)	• Report to EPA and OSHA.
Chemical Bulk Storage (various -EPA, OSHA, States)	• Safe storage and handling of hazardous chemicals and prevention of major accidents (fire, explosion, spills)	No	• Varies	• Report accidental releases and major accidents to state or federal agencies.
Safety and Environmental Management System (Bureau of Safety and Environmental Enforcement (BSEE))	• Assure safety and environmental protection while conducting offshore oil and gas operations.	No	• In developing the JSA for current operations in the facility, previous incidents relevant to the same activity shall be considered.	• Submit to BSEE various reports including EHS Performance reports. • Report of accidents to BSEE.
Chemical Facility Antiterrorism Standard (DHS)	• Prevention of facilities in possession of highly hazardous chemicals from security incidents (terrorist attacks).	Yes - Site Security Plan includes measures to deter cyber sabotage.	• While determining the security risk of the facility, information on the history of facilities is taken into consideration.	• Submit Top Screen, Site Security Plan or Security Vulnerability to DHS. • Report of significant security incidents to DHS and local law enforcement.
Seveso Directives III (EU)	• Control of major accident hazards involving dangerous substances.	No	• The regulation requires facilities to enable public and community to participate in decision making on facility siting, modifications on processes, activities, etc. • The safety report shall include a review of historical accidents with the same substances and processes used and learnings from them.	• Submit the Notification, safety report, MAPP to competent authority of Member States. • Report major accident to competent authority.
COMAH (UK)	• Prevention of major accidents involving dangerous substances and mitigation of their impact in case of occurrence.	No	• The safety report shall include a review of historical accidents with the same substances and processes used and learnings from them.	• Submit COMAH Notification and safety report to competent authority • Report major accident.
NORMA (Mexico) (Example NOM 005-STPS-1998 and NOM-020-STPS-2011)	• Prevention of major accidents during the handling, storage, and transportation of hazardous chemical Substances. • Protection of workers and public from pollutants.	No	• Emergency plans are developed based on the most potential scenarios and taking into account the risk levels as defined in the process information.	• Any modification or change in the process or substances to be reported to the Ministry of Labor and Welfare.
PSM and Safe Management of Hazardous Chemicals regulations (China) Example (Decree 591; AQ/T 3034-2010;AQ/T 3012-2008)	• Safe management of hazardous chemicals and prevention of process-related accidents.	No	• The regulations require to take into account residual risks and past process events in process hazard identification and risk assessment.	• Report to local competent authorities in case of major accident (Safety Production Supervision and Administration, Ministry of Environmental Protection, Ministry of Public Security, and Ministry of Health)

C. Preliminary Data Analysis

Knowing that an IDS (filter) system is analogous to a guard and an incident log, we examined an available cyber filter dataset of email. We extracted and cleaned an available dataset of 40,761,709 events collected over thirty consecutive days from June 27, 2019 to July 29, 2019. There are many limitations to this dataset, namely, it is from a single source email system, with a specific IDS (filter), examines only a limited timeframe and is not a PSM operational network. Nevertheless, the data did allow us to explore the efficacy of hierarchical incident occurrence. Interestingly, the analysis showed that 98% of the events were stopped due to reputation filters, and approximately 1% were invalid receipts, with spam, virus, malicious URLs and content filters representing much less than 1% of the traffic. Further, the results showed that the incident rates generally were within control limits, with few excursions. UCL is the Upper Control Limit for the filter for each type of incident, which represents the level beyond which the filter loses control on the process (fails to prevent the incident). On the figures, 'Max' is the highest number of occurrences for each incident during that period of time. For each type, the interquartile range, first and third quartile, and median are presented. Figure 7 shows comparison on the performance of the filter in controlling spam detected and invalid recipient incidents that occurred during the thirty day period. Figure 8 represents a comparison of the performance of the filter in filtering viruses, messages with malicious URLs, and incidents by content and shows that the filter failed to stop incidents involving invalid recipients where the highest number of occurrences (max) has gone beyond the UCL. The detected spam incidents remained under control (the highest number of detected spam incidents is below the UCL of the filter). While the filter could detect and control viruses and messages with malicious URLs, it may not have performed as well with other questionable content.

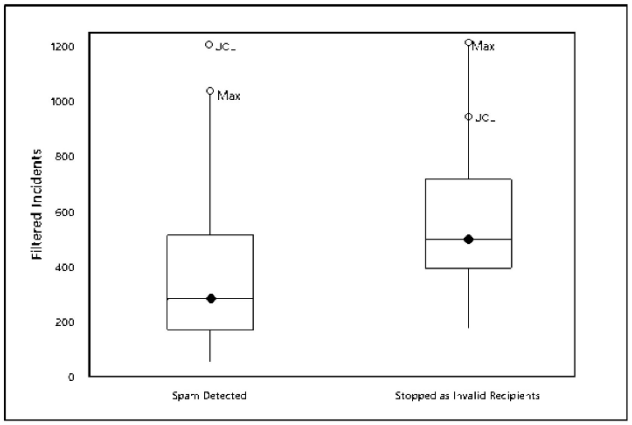

Fig. 7: Filtered intrusion dataset analysis for spam and invalid recipients

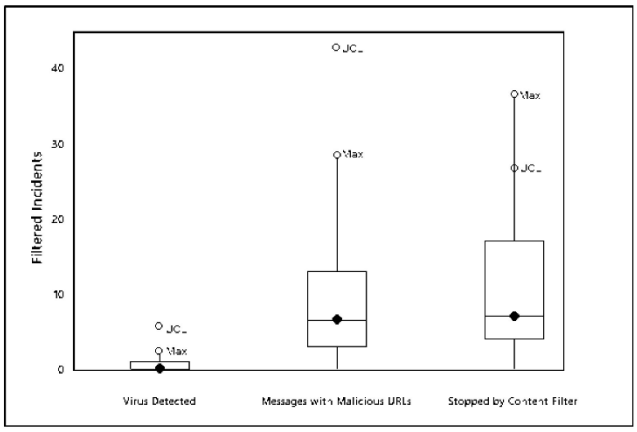

Fig 8: Filtered dataset analysis for virus, malicious URL and content filter

As stated earlier, data is most important in providing situational awareness to identify and resolve unfolding incidents and for after action analysis to improve systems that have been compromised. To that end, this data does not serve that interest, except that the upper control limit excursions are a signal that there may be a material change in the status of the protection system. This dataset also does not include intrusions that were not identified or captured, and thus are dangerous and may propagate further impact in the system, perhaps undetected.

IV. Discussion and Future Work

The data we examined is not a full occurrence dataset, admittedly, it represents incidents that were actually disrupted and does not include event impact. Unlike generalized safety management or specific PSM, there is no source of publicly available validated cyber focused incident data. Casson Moreno, *et al.* [19] extracted 300 cases from nine chemical industry related incident repositories and showed that 11% of PSM reported incidents studied included a cybersecurity actor. This result is likely a small fraction of actual cases. In the last few decades, 'honeypot' models have proliferated in cyber security as a way to attract cyber-attacks and steer them away from truly critical systems. These honeypots are a rich source of cyber incident data, but none are complete [20]. In order to fully understand the distribution and impact of cyber incidents, a repository with appropriate sanitized identifiers needs to be available. Publishing such data may inform those who wish to continue nefarious acts, and it is likely that reputational concerns also prevent publication.

Our cyber data does compare to PSM incident data in that the filter is comparable to an engineering control or 'guard', and each occurrence is a near miss that was mitigated. In that sense, this does show the sheer magnitude of near miss occurrence opportunities that exist in cyber security, and the need to have highly effective mitigations, and attempt to reduce the severity and frequency overall. However, improving controls may not always mitigate severe events as the malicious actor will continue to get smarter and more creative over time. Nevertheless, we have no choice but to continue to do so.

This knowledge can also inform actions across the emergency management arc, and provide more effective response to events, even those occurring outside cyber-systems. Fundamentally, ICT systems are integral to our community's critical infrastructure, including our emergency management processes. The volume of malicious attempts requires highly informed and capable expertise to extract the meaningful information from the noise and the ability to react to it, particularly in emergent situations, whether the community understands the source of the risk or simply the downstream impact, or even if the cyber system is simply the method of transmission of risk.

V. Conclusions

Cyber security risk management is challenging. There are a number of gaps necessary for the field to address as it builds more robust cyber security management systems, and the evolution of process safety risk management systems provides insights for ongoing efforts to achieve more robust cyber security management as part of the critical infrastructure emergency and overall risk management. As many have suggested, effective reporting and collection of cyber incident data is a major step to mitigating these risks, not only for analysis, but also to understand overall occurrence rates [21, 22, 23] and manage these risks. The suite of tools currently available to cyber does reflect typical risk management: access controls based upon approvals (limiting exposure or administrative control), and finally, depending upon the user to ensure security or safety through password protections (protective equipment). As we know, depending upon individual choice introduces human error and relies upon the user to make the right choice. Controls that employ personal responsibility are the least effective, in the same way that passwords, remembered and used by individuals, are also least effective.

As shown in Fig. 1, these steps toward cyber safety and security are not simply for managing risk, but also will become more important as cyber performance and protection becomes an integral consideration of corporate and social responsibility. Microsoft developed a Hierarchy of Cybersecurity Needs that asserts that individuals' cyber

needs extend beyond merely having sustained access to ICT [24], as is the case with many existing social responsibility frameworks, such as ISO 26000:2010 [25] and the Sustainable Development Goals (SDGs) [26]. The Hierarchy developed by Microsoft proposes that companies should seek to first provide access to ICT, but beyond access companies must ensure reliability and predictability, followed by connectivity with other users and trust that their network is secure in order to reach an optimum state of internet usage [24]. As cybersecurity management evolves and transitions away from a reactive approach to a more proactive, socially responsible approach, corporates should consider how they can operationalize this hierarchy to help their customers achieve optimum usage. This will not only improve the company's societal impact, but also is an opportunity to set the company apart from its competitors.

Further research should explore ways in which critical infrastructure may use occurrence- event data to inform layering mitigations and controls to more effectively prevent cyber security incidents. While management system standards currently exist for managing cyber security risks, such as ISO 27031 and NIST 800, [28,29] these standards are focused on managing major information security incidents [6, 7, 8]. Further, though it is difficult to access, examination of actual complete incident databases, including both those events mitigated and those events that completed to a measurable impact would provide further insight into the effectiveness of interventions and inform best practices particularly in emergency management's response and recovery. By proactively striving to achieve cyber resilience, companies can improve community scale connectivity and trust, aspects of social capital (i.e. relationships) that increase community resilience to disturbances [30]. This is similar to the approach more proactive safety management systems employ, and a key component of the corporate social responsibility ideals that ultimately drive risk management.

ACKNOWLEDGMENT

The authors would like to thank colleagues Dr. Sumita Mishra and Dr. Carol Romanowski for their guidance in this work, including data preparation and cyber incident hierarchy creation.

REFERENCES

[1] J. Schneider, C. J. Romanowski, S. Mishra, R. K. Raj and S. Dobie, "Building robust risk management as a method of situational awareness at the local level," 2018 IEEE International Conference for Homeland Security Technology, Woburn, MA, 2018.

[2] J. Schneider, J. Hummel, J. Rosenbeck and S. Dobie, "Community resilience management: reflections and strategies from corporate sustainability," Journal of Environmental Sustainability, vol. 6, no. 1, pp. 15-36, 2018.

[3] Zhong C., Yen J., Liu P., Erbacher R.F., Garneau C., Chen B., "Studying analysts' data triage operations in cyber defense situational analysis," In: Liu P., Jajodia S., Wang C. (eds.) Theory and Models for Cyber Situation Awareness. Lecture Notes in Computer Science, vol. 10030. Springer, Cham (2017) https://doi.org/10.1007/978-3-319-61152-5_6 (Accessed 30 July 2019).

[4] J. Schneider, C. J. Romanowski, R. K. Raj, S. Mishra and K. Stein, "Measurement of locality specific resilience: an operational model," 2015 IEEE International Conference on Technologies for Homeland Security (IEEE HST 2015), Waltham, MA. April 2015.

[5] Department of Homeland Security, Chemical Facility Antiterrorism Standard. https://uscode.house.gov/view.xhtml?path=/prelim@title6/chapter1/subchapter16&edition=prelim (Accessed 2 March 2018).

[6] M. Kuypers, T. Maillart and E. Pate- Cornell, "An empirical analysis of cyber security incidents at a large organization," Stanford Freeman Spogli Institute for International Studies - All FSI Publications 2016. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/kuypersweis v7.pdf. (Accessed 30 July 2018).

[7] J. Cebula and Young, L., "A taxonomy of operational cyber security risks" Carnegie Mellon University - Software Engineering Institute, December 2010. https://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15200.pdf. [Accessed 3 April 2019].

[8] Z. Collier, I. Linkov, D. DiMase S. Walters, M. Tehranipoor and J. Lambert, "Cybersecurity standards: managing risk and creating resilience," Computer, vol. 47.9, pp. 70-76, 2014.

[9] H.W. Heinrich and E.R. Grannis, "Industrial accident prevention: a scientific approach," New York: McGraw Hill, 1959.

[10] S. Rathnayaka, F. Khan and P. Amyotte, "SHIPP Methodology: predictive modeling approach," Process Safety and Environmental Protection, vol. 29, pp. 151-164, 2011.

[11] Y. Li. and F. Guldenmund, "Safety Management Systems: a broad overview of the literature," Safety and Science, vol. 103, pp. 94-123, 2018.

[12] Occupational Health and Safety Administration: Process Safety Management 29CFR1910.120 https://www.osha.gov/laws-egs/regulations/standardnumber/1910/1910.119 (Accessed 2 March 2018).

[13] CCPS − Center for Chemical Process Safety, 2003. "Guidelines for analyzing and managing the security vulnerabilities of fixed chemical sites" http://dx.doi.org/10.1002/9780470925003 (Accessed 3 April 2019).

[14] Safety and Environmental Management System (Bureau of Safety and Environmental Enforcement (BSEE)) https://www.bsee.gov/resources-and-tools/compliance/safety-and-environmental-management-systems-sems (Accessed 3 April 2019).

[15] European Parliament and Council, 2012. Seveso III, Directive 2012/18/UE.

http://extwprlegs1.fao.org/docs/pdf/ire134044.pdf (Accessed 3 April 2019).

[16] Health and Safety Executive, 2015. The Control of Major Accident Hazards Regulations 2015 (COMAH). https://www.hse.gov.uk/comah/background/comah15.htm (Accessed 3 April 2019).

[17] NORMA (Mexico) NOM 005-STPS-1998 NORMA: NOM-020-STPS-2012 https://mexicanlaws.com/STPS/NOM-028-STPS-012.htm (Accessed 3 April 2019).

[18] J. Zhao, J. Suikkanen, and M. Wood, "Lessons learned for process safety management in China," Journal of Loss Prevention in the Process Industries, vol. 29, May 2014, pp.170-176, 2014 https://www.sciencedirect.com/science/article/abs/pii/S0950423014000333 (PSM and Safe Management of Hazardous Chemicals regulations (China) (Decree 591; AQ/T 3034-2010; AQ/T 3012-2008) (Accessed 3 April 2019).

[19] V. Casson Moreno, G. Reniers, E. Salzano, and V. Cozzani, "Analysis of physical and cyber security-related events in the chemical and process industry," Process Safety and Environmental Protection, 116:2018pp.621-631,ISSN0957-5820 https://doi.org/10.1016/ j.psep. 2018.03.026 http://www.sciencedirect.com/science/article/pii/S095758201830079X). (Accessed 3 April 2019).

[20] Nawrocki, M., Wählisch, M., Schmidt, T.C., Keil, C., & Schönfelder, J. (2016). "A survey on honeypot software and data analysis," *ArXiv, abs/1608.06249*. https://arxiv.org/pdf/1608.06249.pdf (Accessed April 4, 2019).

[21] G. Brown, M. Carlyle, J. Salmeron and K. Wood, "Defending critical infrastructure," INFORMS Journal on Applied Analytics, vol. 36, no. 6, pp. 530-544, 2006.

[22] A.L. Joyce, N. Evans, E. Tanzman and D. Israeli, "International cyber incident repository system: information sharing on a global scale," International Conference on Cyber Conflict (CyCon US), Waltham, 2016. http://dx.doi.org/10.1109/CYCONUS.2016.7836618. (Accessed March 21, 2019).

[23] S.A. Elnagdy, M. Qiu and K. Gai, "Cyber incident classifications using ontology-based knowledge representation for cybersecurity insurance in the financial industry," IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), Beijing, 2016. https://ieeexplore.ieee.org/document/7545936 (Accessed 4 April 2019).

[24] Microsoft and Oxford Analytica, "Hierarchy of cybersecurity needs: developing national priorities in a connected world," Nov. 2013.

[25] ISO 26000: 2010 Guidance on social responsibility. Available at https://www.iso.org/standard/42546.html [Accessed 3 October 2019].

[26] United Nations Development Programme, "Sustainable Development Goals," *UNDP*. https://www.undp.org/content/undp/en/home/sustainable-development-goals.html. [Accessed: 27 February 2019].

[27] ISO 37101: 2016 Sustainable development in communities -- Management system for sustainable development -- Requirements with guidance for use. https://www.iso.org/standard/61885.html. (Accessed March 10, 2018).

[28] ISO/IEC 27031: 2011 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity. https://www.iso.org/standard/44374.html. (Accessed March 10, 2018).

[29] Special Publication (NIST SP) - 800 53 Rev 4. https://nvd.nist.gov/800-53. (Accessed March 10, 2018).

[30] E. G. Callaghan and J. Colton, "Building sustainable & resilient communities: a balancing of community capital," Environment, Development and Sustainability, vol. 10, no. 6, pp. 931-942, 2008.