INL/EXT-19-53494-Revision-0

Industrial Control System Risk

Peyton T Price, Mohammed Marufuzzaman

May 2019

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-19-53494-Revision-0

Industrial Control System Risk

Peyton T Price, Mohammed Marufuzzaman

May 2019

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Industrial Control System Risk

Peyton Price
Idaho National Laboratory
Idaho Falls, ID 83415
Email: peyton.price@inl.gov

Mohammed Marufuzzaman
Mississippi State University
Starkville, Mississippi 39759
email:maruf@ise.msstate.edu

***Abstract*—Risk is integrated into all business processes, and leaders work to limit risk to as low as reasonable within their systems. Within Industrial Control System networks, risk is especially challenging due to the second- and third-order effects that an attack can incur. We present a new equation for risk and analyze its appropriateness in determining risk through Monte Carlo methods. We believe that this new equation has merit in allowing leadership to more quickly access and mitigate risk based off factors within the decision maker's control, understanding how capable an attacker may be, how much impact an attack would have on the system, and how intensely an attacker may want to cause damage to the system. These variables will allow a leader to provide strategic vision to the business that he/she leads.**

***Keywords*- industrial control system, risk, network security, monte carlo, impact, opportunity, capability, intent, cyber physical systems.**

I. Introduction

Reducing risk is a major decision point for leaders in all sectors. Risk represents a challenge to ensuring that a business or operation can occur with minimal hazards impeding success. The way that risk is viewed and discussed is driven by leaders who set the tone and agenda for those under their authority [1]. Leaders are best able to assess risk when they are able to use objective assessments, but they must operate their business in a manner that provides them a risk profile that is most comfortable for their operations [2]. Cybersecurity challenges risk decision-making because the domain in which it operates changes at an incredibly high pace. The cybersecurity challenge is amplified when dealing with Industrial Control Systems (ICS). ICS is defined as "supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)" [3]. These devices have long service lives and do not have the same upgrade cycle as a normal business information techonology. When determining risk to an ICS, second- and third-order effects must be reviewed in order to maintain the ability of the identified critical infrastructure to survive and recover from cybersecurity hazards [4].

Our research focuses on presenting risk to ICS in such a way as to best help leaders determine their risk profile and make decisions to assist managers and analysts to best defend the ICS network. We further the research in risk determination by presenting an equation for risk in the context of ICS, analyze the presented equation for appropriateness, and present a method for predicting an attacker's capability to damage an ICS.

Organization: In Sec. II, we discuss risk and present our equation and in Sec. III our methodology for determining attacker capability. In Sec. IV, we analyze the appropriateness of our presented equation, and we conclude in Sec. V presenting future work.

II. Background

There are many different methods to determine risk within ICS [5]–[8]. No matter the methodology, risk is well established as [9]:

$$R = (s_i, p_i, x_i), i = 1, 2, ..., N \tag{1}$$

where s_i is the scenario identifier, p_i is the probability of a identified scenario, x_i is the consequence or impact of the identified scenarios, and N is the number of scenarios. More simply stated, risk is the likelihood that an unwanted event might occur [10].

This generic equation is sufficient for many applications, but National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) define risk within the cybersecurity environment as [3], [11]:

$$R_i = T_i * V_i * I_i \tag{2}$$

where T is threat, V is vulnerability, and I is impact, and i is the device being assessed.

Idaho National Laboratory (INL) and others define threat as a function of opportunity, capability and intent [3], [12]–[14], which for the purpose of this study we modify to be:

$$Threat = Capability * Intent * Opportunity \tag{3}$$

From the above equations, we set our risk equation as:

$$R_s = \frac{\sum_{i=1}^{n} o_i * c_i * imp_i * int_i}{n} \tag{4}$$

where R_s is the risk to the entire system of systems, o_i is opportunity for an attacker on an individual system, c_i is capability of the attacker on an individual system, imp_i is impact to the an individual system, int_i is the intent of the attacker on an individual system, and n is the number of systems in the entire system of systems. We do not include vulnerabilities as a part of the risk equation because while vulnerabilities management is an important part of cybersecurity, it does not completely prevent a determined attacker from gaining access

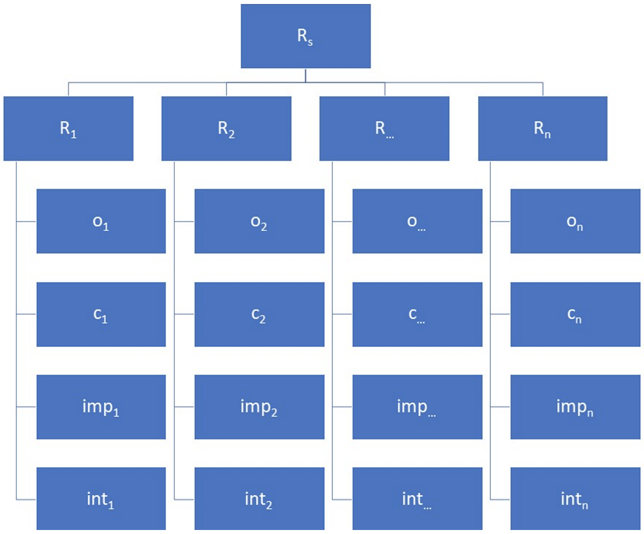

Fig. 1. System of Systems Risk

TABLE I
RISK LEVELS

Risk Level	Risk Scale
Low	$0 \leq R_s < 0.25$
Medium Low	$0.25 \leq R_s < 0.5$
Medium High	$0.5 \leq R_s < 0.75$
High	$0.75 \leq R_s \leq 1.0$

to a system. Therefore, we include vulnerability management as part of our opportunity variable. All values of each variable are normalized between 0 and 1 to allow risk calculations to be expressed as a percentage, and divide by the number of systems to average the risk for the system of systems.

Depending on leader priorities, it may be deemed necessary to weight the importance of each variable. One way the weightings can be garnered is through pair-wise comparison and eigenvector normalization. With weighting, our updated equation becomes:

$$R_s = \frac{\sum_{i=1}^{n}(w_o * o_i) * (w_c * c_i) * (w_{imp} * imp_i) * (w_{int} * int_i)}{n} \quad (5)$$

We further discuss each variable in Subsections II-A – II-D.

As shown in Figure 1, the risk of the system of systems is made up of the sub-components of each the subsystems. It is important to set levels to assist in providing context to the numbers gained from Equations 4 or 5. We define four different risk levels; however, we do not set if each of these levels are better or worse for an ICS. We leave the acceptance of that risk to the leader of the ICS to set the organization's appropriate risk profile. Risk levels are set in Table I.

A. Intent

We define intent as the level of resources and focus an attacker will use to gain access to a system. Given the complexities of the psychology behind determining intent, we leave that to future research and set intent as 1.0.

B. Opportunity

Opportunity, as adapted from [15], [16], is the ability for a defender to make changes to their network to prevent an attack. One method for determining opportunity would be to use Markov Models to predict the change in the security state [17]. Markov models, as presented by [17], are heavily time-dependent and focus on types of attacks tied to vulnerabilities which limits the scope of an attackers available means to attack a system. Common Vulnerability Scoring System (CVSS) scores of vulnerabilities are a main factor in how many track risk to a system [18], [19], including modifying scores to better fit ICS [20], [21]. As mentioned previously, patching vulnerabilities do not stop a determined attacker, and within ICS built-in engineering functions and current protocols allow an attacker to gain complete control of a system without the attacker having any ability to stop the attack [22], [23].

A better method for determining opportunity would be to look at available standards that take into account vulnerabilities, but do not focus solely on them. National best practices, such as NIST or U.S. Government guides [3], [24]–[26], or regulatory requirements, such as NRC Cyber Security Regulatory Guide for Nuclear Facilities or North American Reliability Corporation Critical Infrastructure Protection (CIP) standards [27], [28], provide excellent overall security posture reviews for both physical and cybersecurity. These standards are widely available and used by many organizations already to secure their infrastructure. Opportunity has an inverse relationship with risk. The more controls implemented the greater the overall risk is reduced. We propose using one of the well known standards listed above to calculate opportunity as:

$$o_i = 1 - (\% \text{ of controls implemented}) \quad (6)$$

The opportunity variable should never be zero since not all part of each standard will be able to be implemented due to the system design or use. Just as with all assessments, it is important to be conservative and judicious in the scoring of opportunity, so as not to show the attacker opportunity as less than it is.

C. Impact

Impact is defined as the measure of the damage that an attacker can cause if a malicious action is taken on a system [9]. In ICS risk research, impact is the most well documented due to it being easier to determine post event effects after an event occurs. Fault tree analysis is a risk determination method for determining how a failure can occur through causal chain of events [29]. Cybersecurity and ICS network defense has used fault trees, and their subset attack graphs, to determine impacts on systems [30]–[33]. Fault trees and attack graphs are extremely useful, but quickly become burdensome and overwhelming with a complex system, and a different tree or graph must be created for each identified issue. Another method is to identify impact through looking at economic, social, or insurance loss [34]–[39]. These methods are effective at being easily translatable to a leader, but do not discuss the impact that would have on the ICS's ability to operate. Loss methods are more suited for a retail-style business where loss of financial information may lead to less consumers.

We believe the best method for determining impact is analyzing what is needed for a system to conduct its required operations, or mission. Impact to mission has been looked at by analyzing the effectiveness of devices under degradation [40], which systems are required to maintain mission capability [41], or worst-case scenario, crown jewel analysis that would cripple an ICS business [22], [42], [43]. We propose using the Consequence-driven, Cyber-informed Engineering (CCE), as proposed by INL and [22], [42] to determine the impact score.

D. Capability

Capability is the amount of ability by which an attacker is able to conduct a malicious event on a system [15], [16]. Identifying attacker capability within ICS focuses on creating signatures from honeypots [44], determining the type of attack that is occuring [45], and deploying countermeasures to defeat an ongoing attack [39], [46].

For leadership making risk-based decisions, it is important to be able to predict the attacker's ability to conduct an attack prior to it happening. From our research, there has yet to be a study focusing on predicting attacker abilities prior to attack. In non-ICS research, predictive attacker capability has been conducted by tying vulnerabilities to how likely those vulnerabilities are to be exploited [47], or by using a planning feedback loop to use current operations by an attacker to predict future operations [16].

III. Methodology

We propose having experts set likelihoods of events using a Bayesian network to determine attacker capability. Bayesian networks allow subjective and objective information to be applied and are updated easily when new information is received [48]. They have also been used extensively in risk assessments, ICS safety assessments and cybersecurity defense [49]–[54]. Bayesian networks are better for determining attacker capability than other probabilistic risk assessment methods, such as Markov networks, because they are directed acyclic graphs that have dependencies for when events can occur [55].

As shown in [56], [57], it is possible to predict the likelihood of an event if the order of required events is known. We define our Bayesian network in Figure 2 based off the ICS Kill Chain, as developed by Michael Assante and Robert Lee [58]. The *green* area of Figure 2 can be objectively assessed prior to an attack by an expert, the *yellow* section can possibly be assessed prior to an attack, and the *red* section cannot be assessed until an attack on the system has started. If the attacker reaches the last *red* area, the risk is unacceptable, or 1. We determine the attacker capability from the *green* and *yellow* sections. The full joint probability of Figure 2 is defined as [48]:

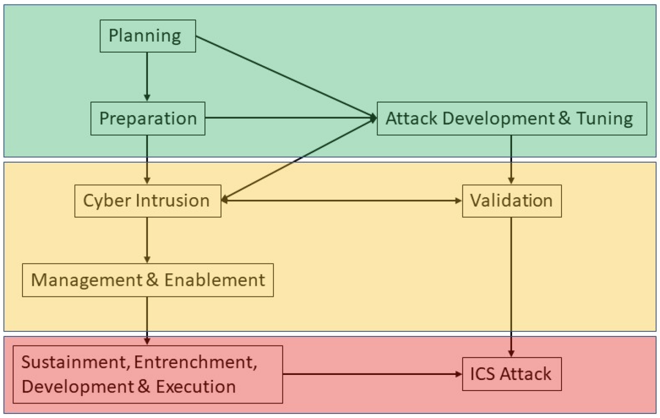
Planning
Preparation
Attack Development & Tuning
Cyber Intrusion
Validation
Management & Enablement
Sustainment, Entrenchment, Development & Execution
ICS Attack

Fig. 2. ICS Kill Chain Bayesian Network

$$P(cap_1, cap_2, cap_3, ..., cap_n) = \prod_{i=1}^{n} P(cap_i \mid cap_{i+1}, ..., cap_n) \tag{7}$$

In order to analyze the suitability of our risk equation (Equations 4 and 5), we conduct Monte Carlo simulations of the opportunity, capability, and impact variables. As a reminder, we treat intent as one, since it is not in our area of research. Monte Carlo simulations use random samples to obtain numerical results and assist in decision making [59].

We insert pseudo-random numbers via the Mersenne Twister algorithm for the opportunity, capability, and impact. We measure the average risk score, standard deviation, minimum iterations required, probability that the risk score falls within each area of our scale (Table I), and the probability that the risk score is greater than 0.50. Our minimum iterations are calculated by the equation [59]:

$$N = \left(\frac{Z_{\alpha/2} * \sigma}{e} \right)^2 \tag{8}$$

where N is the number of iterations, $Z_{\alpha/2}$ is the z-score for confidence from standard normal distribution, σ is the standard deviation, and e is the specified error. For our research, the specified error is 1% or 0.01. We run a minimum of 3000 iterations.

We also run Monte Carlo simulation with each variable limited to above the minimum of each of our risk levels. Random numbers are generated between 0.0–1.0, 0.25–1.0, 0.5–1.0, and 0.75–1.0 for each variable. These variations will work to show effects for when scores of each variable move higher and how the risk score changes. Results and implications from our simulations are discussed below in Section IV.

IV. Analysis and Results

As discussed previously, risk has many ways to be calculated through qualitative and quantitative methods. The main

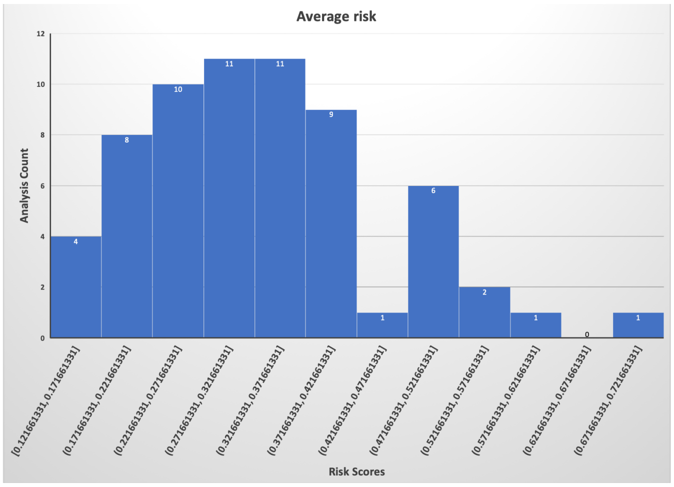

Fig. 3. Histogram of Risk Scores

goal in formulating a risk calculation is to reduce the possibility of a hazard occurring to as low as reasonably allowable to ensure success of the system [29]. For our analysis, we have four variables, of which three variables are being analyzed (opportunity, capability, and impact), and four levels of scores for each variable. We also compare Equation 4 and 5. These factors give 65 possible analyses to compare. We analyze effects on the risk score overall, the effect of weighting on the risk score, and the effect of varying the minimum allowable score for each variable on the risk score in Subsections IV-A – IV-C.

A. Average Risk Score

From the 64 possible analyses from varying Equation 4, the average risk score was approximately 0.33 with a standard deviation of approximately 0.17. The average minimum iterations needed for a 95% confidence interval for our specified error of 0.01 was approximately 1,200 iterations with a low of approximately 800 iterations and a high of approximately 2,100 iterations. Our 3,000 iterations was sufficient to reach a desired error with a 95% confidence interval. Figure 3 shows the distribution of each of the risk scores for each of the 64 analyses.

We can see that approximately 93.75% of all risk scores fall into either *medium low* or *low* risk categories. Specifically, *medium low* risk scores made up approximately 62.5% of all risk scores and are shown in Figure 4. While he lower risk levels might suggest that the risk equation is not effective, we believe they illustrate that appropriately setting the defenses your own network (opportunity variable) reduces the impact of an attack and increases the capability an attacker must have to be successful.

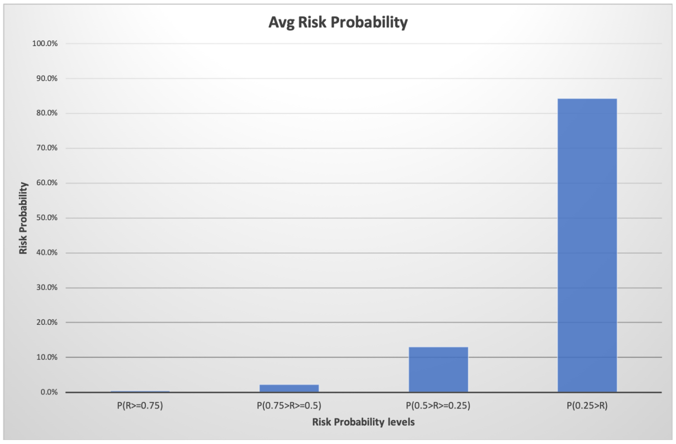

Fig. 4. Histogram of Average Risk Scores for Risk Levels

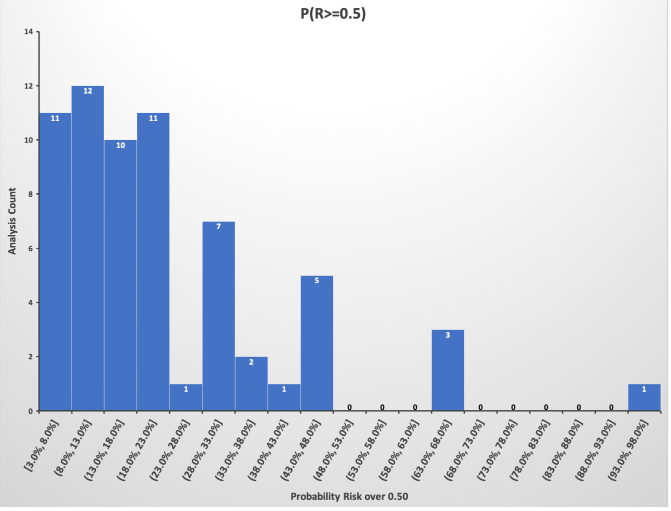

Fig. 5. Histogram of Probability of Risk Scores Greater than 50.0%

Given that leadership will focus on risk scores that are higher, we look at the probability that the risk score will be above 0.50 for each of the 64 analyses. While we do not decide if a 0.50 risk score is positive or negative, we believe that leadership would be less willing to accept risk levels of *medium high* and *high*. None of the analyses has a 0.0% probability of a risk level greater than 0.50. Approximately 84.4% of all analyses have a probability greater than 10.0% of having a risk level of *medium high* or *high*. Having a possibility of a risk level of *medium high* or *high* greater than 10% would cause leadership to want to maximize the ability to limit that potential risk, and would prevent an insurer from insuring against a cyber event as described by [2].

B. Weighting Affects on Risk

We calculate risk score with Equation 5 adding in pseudo-random weights in the same manner as described in Section III. We set the weights and variables between 0.0 and 1.0 and compare the results to the non-weighted risk score with variable values set between 0.0 and 1.0.

The weighted average risk score was approximately 0.0029 with an approximate standard deviation of 0.0040. The minimum required iterations for a 95% confidence interval with

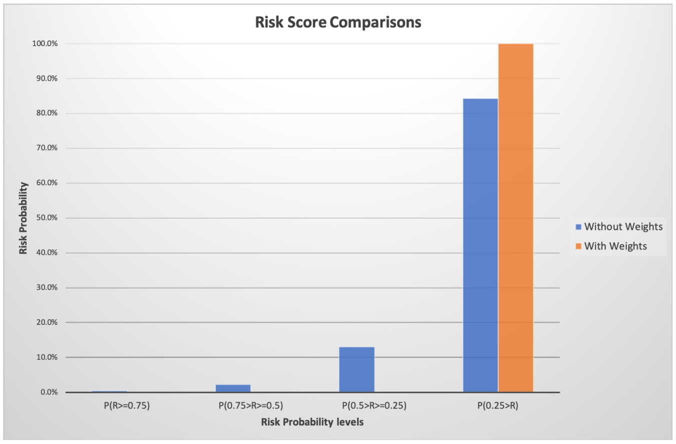

Fig. 6. Weighted v. Non-weighted Risk Scores

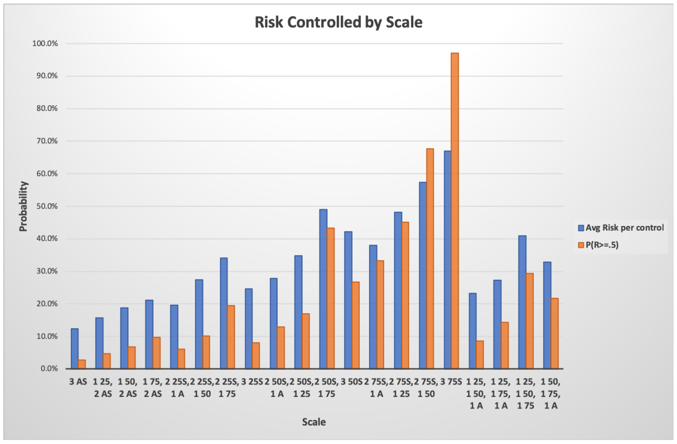

Fig. 7. Risk Controlled by Score Levels

error of 0.01 was one iteration. For the non-weighted average risk score was approximately 0.12 with an approximate standard deviation of 0.14. The minimum required iterations for a 95% confidence interval with error of 0.01 for the non-weighted risk was approximately 784 iterations. We conducted $3,000$ iterations for each equation.

Figure 6 shows the distribution of scores for each risk level. For Equation 5, all (100%) of the risk scores are in the *low* risk level. For Equation 4, approximately 84.4% are in the *low* risk level. Equation 4 has approximately 3.0% of risk scores in either *medium high* or *high* risk levels. Weighting clearly reduces the impact of each variable to the risk score. This reduction in the risk score makes it impractical to assess the risk to the system unless the scaling of the risk score is set up differently. If a leader believes that one of the variables is more important than the others, they should make risk decisions based on the score calculated by that variable.

C. Variable effects on Risk

Given that weightings invalidate the risk score and each variable has equal effect on the risk score, we conduct analysis on how different variable score levels impact the risk score as discussed in the beginning of this Section.

We calculate average weighting and probability that the risk score will be above 0.50 for when each variable has a value: between $0.0 - 1.0$, referred to as *A*; between $0.25 - 1.0$, referred to as *25*; between $0.50 - 1.0$, referred to as *50*; and between $0.75 - 1.0$, referred to as *75*. Within the 64 analyses, there are multiple instances where each variable is set at a particular value. We show all of the different variations of each level in the 64 initial analyses in Figure 7 leading to 20 analyses for variable level control effect.

When controlling for variables, approximately two sets of analyses (*2 75s, 1 50* and *3 75s*) have a risk score averaging above 0.50. Twelve analyses have an average risk level of *medium low*, and six have an average risk level of *low*. When a single variable is changed between levels, it causes approximately a 6.70% change in the risk score overall. Based off of the average risk score in the analyses, an extremely conservative method for calculating the risk score would be to set each variable at the lower end of each scoring level, and then average the scores out. We feel this method may miss out on some of the intricacies for determining the risk of each area, but would allow for quicker analysis and decision making. This simplification would cause risk calculation error if the variable were close to the next high risk score level.

Approximately 7 analyses had a probability of less than 10.0% for a risk score greater than 0.50. Approximately 9 analyses had a probability between 10.0% and 40.0% of risk score greater than 0.50, and four analyses had a probability greater than 40.0%. We consider 65.0% of all analyses having probability greater than 10.0% of having a *medium high* or *high* risk level a significant issue. The range of risk scores and the probability for greater than 0.50 risk score indicates that the Equation 4 has good sensitivity for figuring out the risk of a system. We acknowledge that a weakness of this equation is that each variable must be greater than 0.90 in order to reach a risk level of *high*. We believe that while any one area may have a *high* score level, the other areas are able to reduce the risk level to *medium high* or *medium low*. For example, a system may experience high impact to continued operations if attacked, but if the network and physical security (opportunity) has the applicable defenses in place, and the attacker does not have an attack vector (capability), the risk to the system is greatly reduced. For this reason, we believe that only having a small percentage of scores determined to be as *high* risk level is appropriate.

V. Conclusion

We believe our proposed calculation of risk presented in Equation 4 is suitable for use in determining a risk within ICS. The equation takes into account multiple aspects of security from vulnerability management to security controls (opportunity), the ability of an attacker to conduct an attack (capability), the damage done to a system if attacked (impact), and how intensely an attacker wants to cause damage to a system (intent).

While we only look at the first three and leave intent to others, the analysis of the equation shows sufficient results from Monte Carlo iterations to be useful for leaders looking to make risk decisions. We also acknowledge that some aspects of the equation will be more important for leaders than others. In that case, risk decisions should be made based on the variable deemed most important by the leader, instead of applying weights to the equation.

A. Future Work

Future research will look to further advance the calculation of the variables within the proposed risk equation. Specifically, seeking an answer whether the proposed Bayesian network in Subsection II-D can predict the probability of attack occurrence. We have seen from historical examples that events can be if the chain of events can be known [56], [57]. Both theoretical and case study analysis will be helpful in proving viability of the method.

REFERENCES

[1] J. O. Planning, "Joint publication (JP) 5-0," *Washington, DC: CJCS*, 2017.

[2] A. Coburn, E. Leverett, and G. Woo, *Solving Cyber Risk: Protecting Your Company and Society*. Wiley, 2018.

[3] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Sp 800-82, guide to industrial control systems (ICS) security," 2015.

[4] T. W. House, "Ppd-21: Critical infrastructure security and resilience," Tech. Rep., 2013.

[5] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk asessment methods for scada systems," *Computers & Security*, vol. 56, pp. 1–27, 2016.

[6] L. Shi, Q. Dai, and Y. Ni, "Cyber–physical interactions in power systems: A review of models, methods, and applications," *Electric Power Systems Research*, vol. 163, pp. 396–412, 2018.

[7] M. Roldán-Molina, Gabriela nad Almache-Cueva, C. Silva-Rabadao, I. Yevseyeva, and V. Bast-Fernandes, "A comparison of cybersecurity risk analysis tools," *Procedia Computer Science*, vol. 121, pp. 568–575, 2017.

[8] Y. Peng, T. Lu, J. Liu, Y. Gao, X. Guo, and F. Xie, "Cyber-physical system risk assessment," in *Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference on*. IEEE, 2013, pp. 442–447.

[9] S. Kaplan and B. J. Garrick, "On the quantitative definition of risk," *Risk Analysis*, vol. 1, no. 1, pp. 11–27, 1981.

[10] C. A. Pinto and P. R. Garvey, *Advanced Risk Analysis in Engineering Enterprise Systems*. CRC Press, 2016.

[11] (2019) Iso/iec 27000 family - information security management systems. [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html

[12] P. D. Gasper, "Cyber threat to critical infrastructure," *Idaho National Laboratories http://usacac. army. mil/cac2/cew/repository/presentations/15_Idaho_Natl_Lab_IACS-CI_Threat_2010-2015. pdf Accessed*, 2008.

[13] E. Gelbstein, "Quantifying information risk and security," *ISACA Journal*, pp. 433–438, 2013.

[14] M. Alali, A. Almogren, H. M. Mehedi, I. A. Rassan, and B. M. Z. Alam, "Improving risk assessment model of cyber security using fuzzy logic inference system," *Computers & Security*, vol. 74, pp. 323–339, 2018.

[15] A. Stevenson, *Oxford dictionary of English*. Oxford University Press, USA, 2010.

[16] A. Steinberg, "Open interaction network model for recognizing and predicting threat events," in *Information, Decision and Control, 2007. IDC'07*. IEEE, 2007, pp. 285–290.

[17] C. Xiaolin, T. Xiaobin, Z. Yong, and X. Hongsheng, "A markov game theory-bsed risk assessment model for network information system," in *Computer Science and Software Engineering, 2008 Internation Conference on*, vol. 3. IEEE, 2008, pp. 1957–1061.

[18] W. Wu, R. Kang, and Z. Li, "Risk assessment method for cyber security of cyber physical systems," in *Reliability Systems Engineering, 2015 First International Conference on*. IEEE, 2015, pp. 1–5.

[19] S. Shetty. Cyber risk scoring and mitigation for resilient cyber infrastructure. [Online]. Available: http://ciri.illinois.edu/content/cyber-risk-scoring-and-mitigation-resilient-cyber-infrastructure

[20] QED Secure Solutions and WhiteScope. (2018) Risk scoring system. [Online]. Available: http://riskscoringsystem.com/

[21] C. Bodungen. (2019) Industrial vulnerability scoring system (IVSS). [Online]. Available: http://securingics.com/IVSS/IVSS.html

[22] A. Bochman. (2018, May) Internet insecurity. [Online]. Available: https://hbr.org/cover-story/2018/05/internet-insecurity

[23] R. Lee, J. Slowik, B. Miller, A. Cherepanov, and R. Lipovsky. Industroyer/crashoverride: Zero things cool about a threat group targeting the power grid. [Online]. Available: https://www.blackhat.com/docs/us-17/wednesday/us-17-Lee-Industroyer-Crashoverride-Zero-Things-Cool-About-A-Threat-Group-Targeting-The-Power-Grid.pdf

[24] R. Ross *et al.*, "Nist sp 800-37, revision 1," *Guide for Applying the Risk Management Framework to Federal Information Systems*, 2010.

[25] U. Department of Energy, "Steps to improve cyber security of scada network," 2005.

[26] W. F. Boyer and M. A. McQueen, "Primer control systems cyber security framework and technical metrics," *Report, May*, 2008.

[27] U. NRC, "Regulatory guide 5.71," *Cyber Security Programs for Nuclear Facilities*, 2010.

[28] C. I. P. NERC-CIP, "North american electric reliability corporation."

[29] C. A. Pinto, L. M. Magpili, and R. M. Jaradat, *Operational Risk Management*. Momentum Press, 2015.

[30] E. B. Rice and A. AlMajali, "Mitigating the risk of cyber attack on smart grid systems," *Procedia Computer Science*, vol. 28, pp. 575–582, 2014.

[31] Z. Mohajerani, F. F, M. Jafary, Y. Lu, D. Wei, N. Kalenchits, B. Boyer, M. Muller, and P. Skare, "Cyber-related risk assesment and critical asset identification within the power grid," in *IEEE PES T&D 2010*. IEEE, 2010, pp. 1–4.

[32] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Computers in Industry*, vol. 100, pp. 212–223, 2018.

[33] P. A. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment of scada and dcs networks," *ISA transactions*, vol. 46, no. 4, pp. 583–594, 2007.

[34] P. Radanliev, D. C. De Roure, R. Nicolescu, M. Huth, R. M. Montalvo, S. Cannady, and P. Burnap, "Future developments in cyber risk assessment of the internet of things," *Computers in Industry*, vol. 102, pp. 14–22, 2018.

[35] M. Negrete-Pincetic, F. Yoshida, and G. Gross, "Towards quantifying the impacts of cyber attacks in the competitive electricity market environment," in *IEEE Power Tech Conference*, 2009, pp. 1332–1336.

[36] A. Cook, H. Janicke, R. Smith, and L. Maglaras, "The industrial control system cyber defence triage process," *Computers & Security*, vol. 70, no. 467–481, 2017.

[37] L. Pavlik and L. Lukas, "Pareto anaylsis as a tool for the identification of assets within the organization providing inusrance against cyber risk," in *Military Technologies, 2017 International Conference on*. IEEE, 2017, pp. 361–365.

[38] L. P. Rees, J. K. Deane, T. R. Rakes, and W. H. Baker, "Decision support for cybersecurity risk planning," *Decision Support Systems*, vol. 51, no. 3, pp. 493–505, 2011.

[39] T. R. Rakes, J. K. Deane, and L. P. Rees, "It security planning under uncertainty for high-impact events," *Omega*, vol. 40, no. 1, pp. 79–88, 2012.

[40] S. Musman, M. Tanner, A. Temin, E. Elsaesser, and L. Loren, "Computing the impact of cyber attacks on complex missions," in *Systems Conference (SysCon, 2011 IEEE International*. IEEE, 2011, pp. 46–51.

[41] P. Price, N. Leyba, M. Gondree, Z. Staples, and T. Parker, "Asset criticality in mission reconfigurable cyber systems and its contribution to key cyber terrain," in *Proceedings of the 50th Hawaii International Conference on System Sciences*, January 2017.

[42] S. Berinato and A. Bochman. (2018, May) Case study: Protecting the cheddar. [Online]. Available: https://hbr.org/2018/05/case-study-protecting-the-cheddar

[43] (2019) Open pha. [Online]. Available: https://www.kenexis.com/software/openpha/

[44] E. Bou-Harb, W. Lucia, N. Forti, S. Weerakkody, N. Ghani, and B. Sinopoli, "Cyber meets control: A novel federated approach for resilient cps leveraging real cyber threat intelligence," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 198–204, 2017.

[45] M. A. Bode, S. A. Oluwadare, B. K. Alese, and A. F.-B. Thompson, "Risk anaylsis in cyber situation awareness using bayesian approach," in *Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2015 International Conference on*. IEEE, 2015, pp. 1–12.

[46] S. Mousavian, J. Valenzuela, and J. Wang, "A probabilistic risk mitigation model for cyber-attacks to pmu networks," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 156–165, 2015.

[47] S. J. Yang, S. Byers, J. Holsopple, B. Argauer, and D. Fava, "Intrusion activity projection for cyber situational awareness," in *Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on*. IEEE, 2008, pp. 167–172.

[48] N. Fenton and M. Neil, *Risk Assessment and Decision Analysis with Bayesian Networks*. Crc Press, 2012.

[49] P. Trucco, E. Cagno, F. Ruggeri, and O. Grande, "A bayesian belief network modelling of organisational factors in risk analysis: A case study in maritime transportation," *Reliability Engineering & System Safety*, vol. 93, no. 6, pp. 845–856, 2008.

[50] W. Watthayu, Y. Peng *et al.*, "A bayesian network based framework for multi-criteria decision making," in *Proceedings of the 17th international conference on multiple criteria decision analysis*, 2004.

[51] C.-J. Lee and K. J. Lee, "Application of bayesian network to the probabilistic risk assessment of nuclear waste disposal," *Reliability Engineering & System Safety*, vol. 91, no. 5, pp. 515–532, 2006.

[52] N. Khakzad, "Application of dynamic bayesian network to risk analysis of domino effects in chemical infrastructures," *Reliability Engineering & System Safety*, vol. 138, pp. 263–272, 2015.

[53] T. Sommestad, M. Ekstedt, and P. Johnson, "Cyber security risks assessment with bayesian defense graphs and architectural models," in *2009 42nd Hawaii International Conference on System Sciences*. IEEE, 2009, pp. 1–10.

[54] P. Xie, J. H. Li, X. Ou, P. Liu, and R. Levy, "Using bayesian networks for cyber security analysis," in *Dependable Systems and Networks (DSN), 2010 IEEE/IFIP international conference on*. IEEE, 2010, pp. 211–220.

[55] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Morgan Kaufmann, 1988.

[56] T. H. Kean and L. Hamilton, *The 9/11 Commission Report: Executive Summary*. National Commission on Terrorist Attacks upon the United States, 2004.

[57] P. E. Tetlock and D. Gardner, *Superforecasting: The art and science of prediction*. Random House, 2016.

[58] M. J. Assante and R. M. Lee, "The industrial control system cyber kill chain," *SANS Institute InfoSec Reading Room*, vol. 1, 2015.

[59] M. Beaverstock, A. Greenwood, E. Lavery, and W. Nordgren, *Applied Simulation: Modeling and Analysis Using FlexSim*. FlexSim Software Products, Inc., 2017.