A Stochastic Model of an Industrial Control System Kill Chain

Guillermo A. Francia, III
Center for Information Security & Assurance
Jacksonville State University
Jacksonville, AL, USA
gfrancia@jsu.edu

Tingting Li
Institute for Security Science & Technology
Imperial College London
London, UK
tingting.li@imperial.ac.uk

Chen Feng
Institute for Security Science & Technology
Imperial College London
London, UK
c.feng@imperial.ac.uk

ABSTRACT

In this paper, we present a Semi-Markov Process (SMP) model of an Industrial Control System (ICS) Kill Chain. We develop the steady state probability equations by first examining the embedded Discrete Time Markov Chain (DTMC) sojourn times. Based on published reports of ICS vulnerabilities and an actual case study of a cyber-attack on a number of power stations on the Ukraine power grid, we derive the parameter values for our SMP model. Using these values, we calculate the steady state probabilities of the model and provide insights on the results particularly on the top two ICS security attributes: availability and integrity.

Categories and Subject Descriptors

- Security and privacy~Formal security models

General Terms

Measurement, Performance, Security, Theory

Keywords

Industrial Control Systems, SCADA, ICS Kill Chain, Stochastic Modelling, Semi-Markov Chain, Security Model

1. INTRODUCTION

Industrial Control Systems (ICS) have been widely employed to supervise and control critical infrastructures in various sectors such as supplying and/or controlling essential energy, water treatment, transport, chemicals, and disparate manufacturing processes. ICS typically consist of a combination of software, hardware and operators. The most common components found in ICS are Systems Control and Data Acquisition (SCADA), Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC).

ICS are originally designed as air-gapped networks, but have now become increasingly interconnected with other IT systems and external networks. Whilst offering efficient communication and high throughput, such evolution has also exposed ICS to a growing number of malicious cyber-attacks. Cyber-attacks on ICS could result in unexpected disruption to controlling critical infrastructures and bring harmful physical damage to all living creatures and the environment. There were 245 cyber-attacks on ICS that were reported to ICS-CERT in 2014 [16]; 295 incidents were reported in 2015 [17]. Stuxnet was disclosed in 2010 as the first cyber weapon causing havoc to a large nuclear plant in Iran. Until September 2010, Stuxnet infected approximately 100,000 hosts across over 155 countries. Two more recent examples are the security breach to a German steel mill causing massive damage to the whole plant in 2014 [18] and the cyber-attack against Ukrainian power companies in 2015 leading to power outage and affecting approximately 225,000 customers[6]. Currently the cyber security of ICS has become an increasing concern for government, industry and academia all over the world.

In this paper, we propose a stochastic model to formally express the complete life-cycle of an ICS-targeted attack. We follow the key phases of the ICS Kill Chain [2], which are then formally represented as a Semi-Markov Chain process. The key contribution of this paper is a novel formal model of an ICS Kill Chain which can be used to derive key security and performance indicators for system integrity, resiliency, survivability, availability, and failure.

The rest of the paper is organized as follows: the ICS Kill Chain and a brief introduction to stochastic modeling are described in section 1; section 2 introduces the transition model of the ICS Kill Chain; section 3 shows the formal semi-Markov model and the development of its steady state equations; section 4 presents the derivation of the parameters values; and finally, in section 5, we provide concluding remarks and some future research directions.

1.1 Industrial Control Systems Kill Chain

In [2], an Industrial Control System (ICS) Kill Chain is introduced. This model is adopted from the seminal work by Hutchins, Cloppert and Amin [4] on Cyber Kill Chain™. The Cyber Kill Chain™ is patterned after the military concept of kill chains to gain a better understanding of the adversary's campaign. To better appreciate the relationship between the original Cyber Kill Chain™ and the ICS Kill Chain, we superimposed them in Figures 1, 2, and 3. A description of each phase is attributed to Assante and Lee [2].

1.1.1 Stage One

Planning Phase. In this phase reconnaissance is performed to gauge the strength of the system defenses as well as gather information that may be used to create attack vectors. In ICS, it may also include researching specific control system vulnerabilities that are endemic to the type of infrastructure that is of interest.

Preparation Phase. This phase will include weaponization or targeting. While weaponization involves the crafting of seemingly innocuous files with exploit code to facilitate the advancement of the malicious objective, targeting is the process of prioritizing targets and matching harmful actions that are appropriate to those targets.

Cyber Intrusion Phase. This phase includes the Delivery step, which is used to induce interaction with the system or the user; the Exploit step, which is the process of gaining unauthorized access to the system; the Install step, wherein the adversary installs applications such as backdoors to be able to gain unimpeded access to the system; and the Modify step, wherein the adversary changes the system environment using existing tools such as PowerShell to be able to escalate system privileges.

Management and Enablement Phase. In this phase, the adversary establishes command and control (C2) using the tools and applications that were successfully installed or built in the previous phase. More often than not, the established C2 will be configured with stealth communication features to prevent detection.

Sustainment, Entrenchment, Development, and Execution. This phase is when malicious actions start to take place. Covert capture of user credentials, lateral movement, data collection and exfiltration, installation of advanced tools, and anti-forensic activities are initiated.

1.1.2 Stage Two

Attack Development and Tuning. This phase may take longer than the other phases. This is the time in which the adversary would take time in developing the suitable attack method and tools based on the exfiltrated data gathered during the previous phases.

Validation Phase. This is when the attacker would test the developed capabilities on a similar system. Activities in this phase would reveal the extent of how much the attack could inflict on the target system.

ICS Attack. In this step, the capability is delivered, installed, and executed.

1.2 Stochastic Modelling

A stochastic model expresses the uncertainty of security posture due to incomplete knowledge by actors on both sides: the adversary and the system designer or operator. In developing the model, probabilities and cumulative distribution functions are used to describe the events that trigger transitions to different states.

1.2.1 Markov Chain

The application of Markov chain model requires the stochastic process to be discretized into a number of states and determining the transition probabilities between two states. In [19], a formal definition of a Markov chain is provided as follows:

Let $X(t)$ be a discrete-state stochastic process and let $Pr(X(t_n) = j)$ be the probability that the process is in state j at the time t_n. $X(t)$ is a Markov chain if, for any ordered times $t_1 < t_2 < \ldots < t_n$, the conditional probability of being in any state j such as that $Pr\{X(t_n) = j \mid X(t_{n-1}) = i_{n-1}, X(t_0) = i_0\} = Pr\{X(t_n) = j \mid X(t_{n-1}) = i_{n-1}\}$.

Essentially, it asserts that any state depends on the state immediately prior to it and cannot depend on any state before that prior state.

In real cyber-attack events, the sojourn time in a particular state may not at all be exponentially distributed but may be described by any arbitrary distribution function. Thus, we use a *semi-Markov process* in which the rate of transition from one state to another may depend on the sojourn time in the source state but not on anything that happened prior to reaching that source state.

Figure 1 Lockheed Cyber Kill Chain

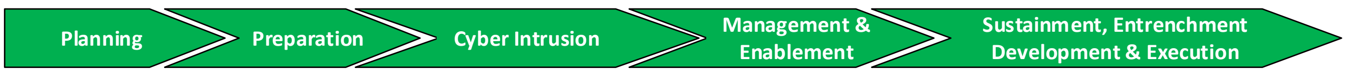

Figure 2 SANS Stage One ICS Kill Chain

Figure 3 SANS Stage Two ICS Kill Chain

Because of the immense variety of attacks, an assortment of distribution functions may need to be considered. In [8], Madan et al. suggest the appropriate distribution function that is suited to a specific threat situation as follows: a hypo-exponential distribution to model transitions involving multi-stage activities and threat situations that may cause monotonically increasing failure rate; a hyper-exponential distribution function to model threats that exhibit a monotonically decreasing failure rate; a Weibull distribution function to model constant failure rate, a monotonically increasing failure rate , or a monotonically decreasing failure rate; and a log-logistic type of distribution function for a combination of decreasing rate of success initially followed by an increasing rate (or vice-versa)[7].

2 The State Transition Model for the ICS Kill Chain

Using the ICS Kill Chain as a basis, we derive a state transition model as shown in Figure 4. Each node represents a state which may comprise of one or more steps on the kill chain. The labelled arcs represent a transition between states. This model will later be transformed into a formal Semi-Markov process chain with steady-state and transition probabilities.

The **Normal state, G**, represents a condition in which the ICS is in normal operating condition. The transition to the **Detect state, D**, denotes the detection/notification of abnormal system behavior, a system patch, or firmware update which may or may not cause any disruption. At some point in time, the ICS transitions to the **Recon state, R,** this is the first step on the ICS Kill Chain.

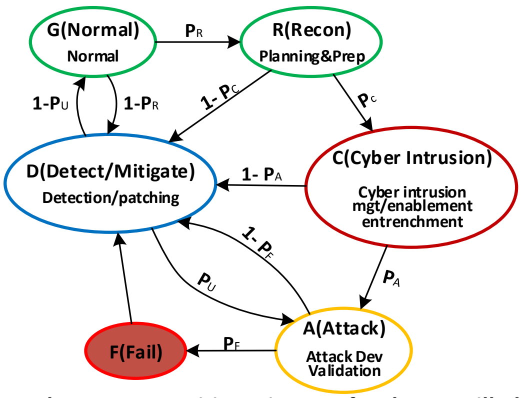

Figure 4 The State Transition Diagram for the ICS Kill Chain

The **Recon state, R**, embodies the reconnaissance, planning, weaponization and/or targeting phase of the chain. If one or more these activities are detected, the model transitions to the **Detect state, D**. An example of such transition occurs when a network mapping or a persistent port knocking activity is discovered. Alternatively, the transition will take it to the **Cyber Intrusion state, C.**

In the **Cyber Intrusion state, C,** the delivery of weaponized documents is made, the command and control system is enabled, and the enhancement of system control and familiarization is accomplished through lateral movements and credential harvesting. A transition to the **Detect state, D, is** made when an activity associated with cyber intrusion is detected. Alternatively, the adversary may decide to enter the attack phase of the kill chain. This is represented by the transition to the **Attack state, A**, of the model.

In the **Attack state, A,** the activities of the adversary may not all happen on the targeted ICS system. With sophisticated or state-sponsored adversaries, the development and validation of the system tools may be conducted at remote systems that mimic the actual target. We assume that some of the activities in this phase will be conducted at the target ICS system infrastructure. When such activity is detected, the model shifts to the **Detect state, D**. Again, an alternative will take it to the **Failed state, F.**

The **Failed state, F**, represents the condition when the full capability of the adversary is delivered, installed, and executed. We assume that the time spent in this state will be minimal as shown by published accounts of several attacks on ICS environment. However, the consequences are far reaching and expensive. After a short time in the state, the model transitions to the **Detect state, D,** for repair, recovery, and other incident response measures.

The **Detect state, D**, is a transition destination of five states: **G, R, C, A, and F**. Essentially, when an abnormal or malicious activity is detected in one of those states, the transition to leave the state is activated. Aside from detection, the repair, patching, recovery and other incident handling activities are performed at this state. Note the existence of a transition from this state back to the **Attack state, A**. This transition embodies the fact that patches and other immediate mitigation tools may not be immediately available. Thus, the prospect of bringing back the system to the **Attack state** is enabled.

3 SEMI-MARKOV PROCESS MODELLING

Formally, we describe the Semi-Markov Process (SMP) as follows: Let $\{X(t) : t \geq 0\}$ be the base stochastic process with a set of discrete state space $X_s = \{A, C, D, F, G, R\}$ with sojoun time distributions, $H_i(t)$ and parameters: h_i , as the sojourn time in **state i** $\in X_s$ and the transition probabilities p_{ij} between states **i** and **j**, where $i, j \in X_s$. At the instants of state transitions, a semi-Markov chain behaves like a Markov chain. Hence, at those instants we have an embedded discrete-parameter Markov chain [10].

Table 1 The ICS Kill Chain Semi-Markov Model Parameters

h_A	Mean time for the ICS to stay in the state of being attacked
h_C	Mean time for the ICS to remain in a compromised state
h_D	Mean time for the ICS to remain in detection, mitigation, and repair state
h_F	Mean time for the ICS to remain in the failed state
h_G	Mean time for the ICS to stay in a normal state
h_R	Mean time for the ICS to stay in the reconnaissance, planning, and preparation state
P_A	Probability of being in the attack state
P_C	Probability of being compromised
P_F	Probability of system failure
P_R	Probability of moving to the reconnaissance/planning state
P_U	Probability of an unmitigated/un-repaired vulnerability
$1 - P_A$	Probability of detecting a cyber intrusion
$1 - P_C$	Probability of detecting a reconnaissance or system mapping
$1 - P_F$	Probability of detecting or mitigating a vulnerability/impending attack
$1 - P_U$	Probability of successful mitigation/patch/repair

Using a similar analysis on the semi-Markov process found in [10], we compute the steady state probability vector **[**$\pi_A, \pi_C, \pi_D, \pi_F, \pi_G, \pi_R$**]** by first computing, for each state, the mean sojourn time

$$h_i = \int_0^\infty (1 - H_i\ (t))\, dt$$

Next we find the steady state $\Gamma = [\gamma_A, \gamma_C, \gamma_D, \gamma_F, \gamma_G, \gamma_R]$ for the embedded discrete-parameter Markov chain by solving the linear system of Equations:

$$\Gamma = \Gamma \times \mathbf{P}$$

$$\Gamma \times \mathbf{e} = \mathbf{1} \text{ or simply } \sum_i \gamma_i = 1, \forall\, i \in \{A, C, D, F, G, R\} \qquad (1)$$

Where **P** is the discrete Markov-chain probability matrix and **e** = **(1, 1, 1, 1, 1, 1)**^{T} **.** Finally, we can compute the steady-state probabilities for the SMP using

$$\pi_i = \frac{\gamma_i \times h_i}{\sum_j \gamma_j \times h_j} \qquad \forall\, i, j \in \{A, C, D, F, G, R\}$$

where the semi-Markov transition is from state **j** to state **i**. For a detailed derivation of the preceding equations, the interested reader is referred to the works of Sahner [10] and Trivedi [19].

The parameters for the SMP are enumerated in Table 1. The transition probability matrix **P** describes the state transition probabilities between the embedded DTMC states shown in Figure 4. The steady-state probabilities of the DTMC, $\Gamma = [\gamma_A, \gamma_C, \gamma_D, \gamma_F, \gamma_G, \gamma_R, \gamma_M]$, are calculated using the following system of linear equations from (1):

$$\gamma_A = \gamma_C P_A + \gamma_D P_U$$

$$\gamma_C = \gamma_R P_C$$

$$\gamma_D = \gamma_R (1 - P_C) + \gamma_C (1 - P_A) + \gamma_G (1 - P_R) + \gamma_A (1 - P_F) + F$$

$$\gamma_F = \gamma_A P_F$$

$$\gamma_G = \gamma_D (1 - P_U)$$

$$\gamma_R = \gamma_G P_R$$

$$\gamma_A + \gamma_C + \gamma_D + \gamma_F + \gamma_G + \gamma_R = 1 \qquad \text{(Equations 3-9)}$$

Solving for the steady-state probabilities of the DTMC in terms of the transition probabilities using Matlab®'s Symbolic Math Toolbox [9] yields equations (10)-(15) as shown in the Appendix. Using equations (10)-(15), we can now calculate the SMP steady-state probability for each state. Henceforth, equations (16)-(21), as shown in the Appendix, are derived.

3.2 Passage Time Analysis

Another measure of interest is that on passage-time distributions. A passage time is a random variable describing the amount of time it takes to reach a state j, given that the process starts in states i. Hence, for the analysis we must assume that target state j is an absorbing state, i.e. states with no outgoing transitions, so that we actually stop measuring the time of a trajectory once we reached the target state. From passage-time distributions we can derive metrics such as mean time to detection (**MTTD**) which is the average passage time from the Normal state, **G,** to the Detect state, **D.** Mean time to compromise (**MTTC**) is the average passage time from Normal state, **G**, to Compromise state, **C.** Mean time to failure (**MTTF**) is the average passage time from Normal state, **G**, to Fail state, **F**. Mean time to recover (**MTTR**) is the average passage time from Compromise state, **C,** to Normal state, **G**. In section 4.4, we present the results of computing the passage-time distributions by gathering samples from multiple simulation runs.

4 DERIVING PARAMETER VALUES

In order to create a model that will represent the system as realistically as possible, we derive values for the sojourn time value for each state *i* and provide justification based on an actual event and other published reports.

4.1 The Cyber Attack on the Ukrainian Power Grid: A Case Study

In December, 2015 a regional electricity distribution company in Ukraine was subjected to a cyber-attack resulting in several power outages that lasted for three hours [6]. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) cited public reports that the BlackEnergy (BE) malware was found on the companies' network but would not confirm its role in the attack [5].

The Ukrainian Power Grid (UPG) cyber-attack demonstrated an adversary that is extremely capable and highly resourced. Several evidence materials point to the fact that the adversary has been conducting long-term planning and reconnaissance, lasting at least six months [13], to be able to execute a highly coordinated and effective attack. Among the technical components used by the adversary are spear phishing, theft of credentials, use of Virtual Private Networks (VPN), use of remote access tools to manipulate Human Machine Interfaces (HMIs), firmware level disruption of devices, utilization of KillDisk , and telephone denial-of-service [6]. The ICS Kill Chain mapping to the UPG cyber-attack is well articulated in [6] and is recapitulated in the following:

The **Reconnaissance** in stage 1 took place at least six months before the actual attack. Evidence reveals that this is a directed attack and that the levels of automation on the distribution systems made them attractive targets.

In the **Weaponization** and/or **Targeting** step at stage 1, the adversary crafted Microsoft Office documents with embedded BlackEnergy malware as attack vectors.

During the **Cyber Intrusion** step at stage 1, the weaponized documents were delivered to individuals working in the administrative and IT sectors of the companies. When the documents were opened, the embedded macros were unleashed which enabled the installation of the BlackEnergy malware. The malware facilitated the command and control communication between the adversary at a remote site and the infected systems within the companies' premises. It is also at this step when credentials were harvested and lateral movement within the IT infrastructure was carried-out.

The **Develop** step in stage 2 occurred mostly within the adversary environment to minimize detection. This step included the design and implementation of malicious tools, both software and firmware, to gain control of the Distribution Management Systems (DMS) and the serial-to-ethernet devices. The **Validation** step in stage 2 was conducted on the adversary site to evaluate and test the malicious tools before the actual attack. These fine-tuned malicious tools were then delivered to the compromised systems before the execution of the actual attack.

During the last step of the ICS Kill Chain, the **ICS Attack,** the adversary utilized the HMIs to manipulate the breakers in the SCADA environment. This opening of breakers enabled 27 substations to be taken offline causing power interruption to more than 225,000 customers. At the same time, the malicious firmware was uploaded to the serial-to-ethernet devices and thereby disabling them for remote control. To exacerbate the situation, a telephonic denial of service on the companies' call centers was initiated to prevent customers from contacting customer support. The entire Kill Chain operation transpired commencing in March 2015 until December 2015.

The purpose of describing the above case study is to provide the reader a grasp of the timeline in which each of the steps in the Kill Chain has occurred. The discussion also facilitates a segue to the derivation of the values for the DTMC sojourn times.

4.2 Industrial Control Systems Vulnerability Statistics

In a 2016 report, Kaspersky lab published a report [1] indicating that there are a total of 189 vulnerabilities in ICS components in 2015. Out of this total number of vulnerabilities, 26 have associated exploits. The report also includes an alarming statistic that patches and/or new firmware are available to only 85% of the published vulnerabilities. Of the remaining 15%, five percent were partially fixed, two percent were unpatched and removed, three percent were unpatched and declared obsolete and five percent remained unpatched. Using this data and using Polityuk's model [11], we calculate a mean sojourn time in the Compromised (C) state of our SMP model to be 24 hours.

4.3 The Parameter Values

Tables 2 and 3 depict a summary of our findings.

Table 2. The Mean Sojourn Time

Sojourn Time	Description	Value (days)	Source
h_A	Mean time for the ICS to stay in the state of being attacked	180	Actual duration of attack (6 months) as reported in the "Analysis of the Cyber Attack on the Ukrainian Power Grid" [6].
h_C	Mean time for the ICS to remain in a compromised position	1	McQueen's model [11] and data from Kaspersky lab report [1]
h_D	Mean time for the ICS to remain in detection/mitigation/patching state	54	2016 Cost of Cyber Crime Study & the Risk of Business Innovation [14]
h_F	Mean time for the ICS to remain in the failed state	0.125	Actual duration of failure reported on the "Analysis of the Cyber Attack on the Ukrainian Power Grid " [6].
h_G	Mean time for the ICS to stay uncompromised in the presence of vulnerability	365	Estimated as 365 days.
h_R	Mean time for the ICS to stay in the reconnaissance, planning, and preparation state	90	Estimated based on the report "Analysis of the Cyber Attack on the Ukrainian Power Grid" [6].

Table 3. Transition Probabilities of the SMP

Transition Probability	*Description*	*Value*	*Source*
P_A	Probability of being attacked	0.70	Miscellaneous published reports
P_C	Probability of being compromised	0.10	Estimated using the Analysis of the "Cyber Attack on the Ukrainian Power Grid" [6].
P_F	Probability of failure	0.15	Estimated using the "Analysis of the Cyber Attack on the Ukrainian Power Grid" [6] and the 2016 Kaspersky lab report [1].
P_R	Probability of being targeted	0.99	Estimated using the "Analysis of the Cyber Attack on the Ukrainian Power Grid " [6].
P_U	Probability of an unmitigated/un-repaired vulnerability	0.05	Estimated using the Analysis of the "Cyber Attack on the Ukrainian Power Grid" [6].

4.4 Interpretation of Results

Using the derived steady-state equations (16)-(21) for the SMP and the data gathered in Tables 2 and 3, we calculated the following steady state probabilities:

$$\pi_A = 0.03912$$

$$\pi_C = 0.000176$$

$$\pi_D = 0.10132$$

$$\pi_F = 0.00000176$$

$$\pi_G = 0.68481$$

$$\pi_R = 0.1588113$$

Furthermore, we also obtained from the simulations of passage time distributions the following results: **MTTD** = 459±7, **MTTC**=5117±99, **MTTF**=29009±555, **MTTR**=194±3 with 95% confidence interval using 10,000 simulation runs.

Based on the above results, we provide the following observations:

a. The steady state probability values suggest the dominant stay of the ICS in the Normal (G), Recon (R) and Detect (D) states. This result clearly validates the Ukraine Power Grid report [6].

b. The almost negligible probability and yet, highly consequential effect, of being in the failed state indicates a highly sophisticated adversary that can produce a significant loss within a short duration.

c. The ***System Availability, calculated as*** 1- π_F **= 0.999996,** remains at a high level despite the fact that the ICS is, at times, in compromised and attack states. The metric indicates the level with which the system is delivering its mission free from degradation or impairment.

d. The ***System Integrity*, calculated as $\pi_G + \pi_R = 0.8436$,** indicates a good amount of time that the system is performing its intended functions without being compromised or manipulated.

5 CONCLUSIONS and FUTURE WORKS

A stochastic model of an industrial control system Kill Chain is designed and applied using parameter values derived from data gathered from an actual case study and currently available published reports. Using the results that were gleaned from calculations using equations derived from the model, we were able to produce the following important ICS security and performance metrics: system availability, system integrity, MTTF, MTTD, MTTC, and MTTR.

A meta-model of cyber physical system attacks referred to as a cyber-physical kill-chain is introduced in [3]. It would be an interesting extension to this study the application of the SMP model to that cyber-physical chain. Further, we recognize that the stochastic model described above requires additional validation using empirical data and robust simulation. Thus, we offer the following future research directions:

- Perform a sensitivity analysis on the model using various sets of parameter values;
- Continue to gather data from actual field reports and use those to validate the model; and
- Design and implement computer simulations to study the effect of various distribution functions on the model.

6 ACKNOWLEDGMENTS

This work is supported in part by grants from the National Science Foundation (Grant Award 1515636), the US-UK Fulbright Commission, the EPSRC project RITICS: Trustworthy Industrial Control Systems (EP/L021013/1), and the EPSRC project: Security by Design for Interconnected Critical Infrastructures (EP/N020138/1). Opinions, findings, and conclusions expressed are those of the authors and not necessarily of the granting agencies.

7 REFERENCES

[1] O. Andreeva, S. Gordeychik, G. Gritsai, O. Kochetova, E. Potseluevskaya, S. I. Sidorov, and A. A. Timorin, "Industrial Control Systems Vulnerabilities Statistics," Kaspersky Website URL: https://kasperskycontenthub.com/securelist/files/2016/07/KL_REPORT_ICS_Statistic_vulnerabilities.pdf. Access Date: February 20, 2017. 2016.

[2] M.J. Assante, R.M. Lee, "The Industrial Control System Cyber Kill Chain" SANS Institute, October 2015.

[3] A. Hahn, R.K. Thomas, I. Lozano, and A. Cardenas, "A multi-layered and kill-chain based security analysis framework for cyber-physical systems" *International Journal of Critical Infrastructure Protection*, vol. 11, pp. 39-50, 2015. http://dx.doi.org/10.1016/j.ijcip.2015.08.003.

[4] E. Hutchins M. Cloppert R. Amin "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11). pp. 113-125 2011.

[5] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), "Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure" Website URL: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01. February 25, 2016.

[6] R. M. Lee, M.J. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid." SANS Industrial Control Systems Website. URL: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdfMarch 18, 2016. Last Access: February 20, 2017.

[7] B. B. Madan, K. Goseva-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, "Modeling and Quantification of Security Attributes of Software Systems." Proc. Of the International Conference on Dependable Systems and Networks (DSN'02). Pp. 505-514. 2002.

[8] B. B. Madan, K. Goseva-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, "A method for modeling and quantifying the security attributes of intrusion tolerant systems." *Performance Evaluation*, vol. 56, no. 1-4, pp. 167-186, 2004.

[9] Mathworks®, "Symbolic Math Toolbox", Website URL: https://uk.mathworks.com/products/symbolic/features.html#linear-algebra. 2016.

[10] R.A. Sahner, K.S. Trivedi, A. Puliafito, "Performance and Reliability Analysis of Computer Systems: an Example-Based Approach Using the SHARPE Software Package," Kluwer Academic Publishers (1996).

[11] McQueen, M., Boyer, W., Flynn, M., Beitel, G.: Time-to-Compromise Model for Cyber Risk Reduction Estimation. In: First Workshop on Quality of Protection (2005).

[12] McQueen, M., Boyer, W., Flynn, M., Beitel, G.: Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System. In: Proc. of the 39th Annual Hawaii International Conference on System Sciences (HICSS) (2006).

[13] Polityuk, P., "Ukraine sees Russian hand in Cyber attacks on power grid" Reuters Technology. Website URL: http://mobile.reuters.com/article/idUSKCN0VL18E. February 12, 2016.

[14] Ponemon Institute, "2016 Cost of Cyber Crime Study & the Risk of Business Innovation," Website URL: https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-8392enw.pdf. October 2016.

[15] Symantec, "Dragonfly: Cyberespionage Attacks Against Energy Suppliers," Website URL: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf. 2014.

[16] ICS-CERT, "ICS-CERT Monitor September 2014-February 2015", https://ics-cert.us-

cert.gov/monitors/ICS-MM201502". Access Date: March 06, 2017.

[17] ICS-CERT, "NCCIC/ICS-CERT Year in Review", https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf", 2015. Access Date: March 06, 2017.

[18] R. Lee, M. Assante, and T. Connway, "ICS cyber-to-physical or process effects case study paper–german steel mill cyber attack," Sans ICS, Dec, 2014.

[19] K. Trivedi, *Probability and Statistics with Reliability, Queuing, and Computer Science Applications* (2nd ed.). John Wiley & Sons, 2001.

8 APPENDIX

Equations (10-15):

$$\gamma_G = \frac{1 - P_U}{2 + P_R + P_U[P_F - P_R] + P_C P_R[1 - P_U] + P_A P_C P_R[1 + P_F - P_U - P_F P_U]}$$

$$\gamma_R = \frac{P_R(1 - P_U)}{2 + P_R + P_U[P_F - P_R] + P_C P_R[1 - P_U] + P_A P_C P_R[1 + P_F - P_U - P_F P_U]}$$

$$\gamma_C = \frac{P_C P_R(1 - P_U)}{2 + P_R + P_U[P_F - P_R] + P_C P_R[1 - P_U] + P_A P_C P_R[1 + P_F - P_U - P_F P_U]}$$

$$\gamma_A = \frac{P_U + P_A P_C P_R - P_A P_C P_R P_U}{2 + P_R + P_U[P_F - P_R] + P_C P_R[1 - P_U] + P_A P_C P_R[1 + P_F - P_U - P_F P_U]}$$

$$\gamma_F = \frac{P_F[P_U + P_A P_C P_R - P_A P_C P_R P_U]}{2 + P_R + P_U[P_F - P_R] + P_C P_R[1 - P_U] + P_A P_C P_R[1 + P_F - P_U - P_F P_U]}$$

$$\gamma_D = \frac{1}{2 + P_R + P_U[P_F - P_R] + P_C P_R[1 - P_U] + P_A P_C P_R[1 + P_F - P_U - P_F P_U]}$$

Equations (16-21):

$$\pi_G = \frac{h_G[1 - P_U]}{h_D + h_G[1 - P_U] + h_R P_R(1 - P_U) + h_C P_C P_R(1 - P_U) + h_A[P_U + P_A P_C P_R - P_A P_C P_R P_U] + h_F P_F[P_U + P_A P_C P_R - P_A P_C P_R P_U]}$$

$$\pi_C = \frac{h_c[P_C P_R (1 - P_U)]\pi_G}{h_G}$$

$$\pi_A = \frac{h_A[P_U + P_A P_C P_R - P_A P_C P_R P_U]\pi_G}{h_G}$$

$$\pi_D = \frac{h_D \pi_G}{h_G}$$

$$\pi_F = \frac{h_F P_F[P_U + P_A P_C P_R - P_A P_C P_R P_U]\pi_G}{h_G}$$

$$\pi_R = \frac{h_R P_R[1 - P_U]\pi_G}{h_G}$$