A Comprehensive and Open Framework for Classifying Incidents Involving Cyber-Physical Systems

William B. Miller
Brigham Young University
Bill_Miller@byu.edu

Dale C. Rowe
Brigham Young University
Dale_Rowe@byu.edu

Richard Helps
Brigham Young University
Richard_Helps@byu.edu

Ross Woodside
Brigham Young University
rossnwoodside@gmail.com

Abstract

In recent years, events such as the Stuxnet nuclear plant cyber-attack have brought the security of industrial control systems under scrutiny. Most of this focus has been on supervisory control and data acquisition (SCADA) systems (more generically known as ICS or industrial control systems). While these systems play a major role in our daily lives, this focus tends to overlook the broader scope of cyber-physical systems (CPS) and the impact they have on human lives (e.g., vehicles, mobile devices, agriculture). There are currently no open databases to record and classify CPS incidents that include systems outside of ICS. While it may be possible to adapt existing databases, we have found that those suitable for adaptation have multiple drawbacks, including proprietary ownership, requirement of a paid subscription and/or limited access, and design scope.

In this paper, we propose an open standards framework for classifying a wide variety of CPS incidents. As part of this framework, we introduce a new taxonomy that facilitates the rapid categorization of such incidents by a variety of criteria. An important new parameter of this taxonomy is a hierarchy of market sector classifications, allowing incidents to be evaluated in their application of context. Other factors of the taxonomy include source profile, impact (both direct and indirect), method, and a comprehensive victim profile. We compare our framework to other existing approaches by classifying several incidents occurring over the last twenty years and demonstrate the wide capabilities of our method by including incidents outside of industrial control systems. We further note that the flexibility of the framework caters for multiple CPU types and provides a context rich description of incidents. Finally, we note that the system allows multiple classifications so an incident can be identified in multiple relevant contexts.

Proceedings of The 2014 IAJC/ISAM Joint International Conference
ISBN 978-1-60643-379-9

We also announce the availability of an online implementation of this framework. This system is intended to be free and cater to an international audience. It is our hope that this will enable researchers to rapidly identify and correlate key incidents involving CPS systems and that, in turn, this will lead to an increased overall awareness of risk management options for these types of systems. We also discuss the security risks involved with making such a framework available and the associated countermeasures we have taken.

Introduction

Incidents such as the SQL Slammer infection at the Davis-Besse nuclear power plant and the Stuxnet attack on the Iranian nuclear facility at Natanz have alerted the industrial community to the need to pay more attention to the security of their critical infrastructure. Most of this focus has been on industrial control systems (ICS), particularly supervisory control and data acquisition (SCADA) systems. In 2012, an attempt was made to classify several incidents involving SCADA [1]. In this process, it was discovered that these types of incidents apply to the broader scope of cyber-physical systems and that a standardized incident classification system is needed. Such a system will allow us to study how incidents happened and what their ultimate effect was.

In this paper, we propose an open standards framework for classifying a wide variety of incidents within cyber-physical systems (CPS). As part of this framework, a new taxonomy has been developed which facilitates the rapid categorization of incidents by a variety of criteria. We demonstrate the utility of our framework by classifying several incidents from ICS and from the broader realm of CPS.

Literature Review

There have been many attempts to define a system for classifying cyber-attacks or incidents. These began as attempts to identify software vulnerabilities that could be compromised to form an attack. In 1998, Howard and Longstaff presented the first attempt at unified security taxonomy. This taxonomy attempted to define an attack based on the tool used, the vulnerability exploited, the action taken, the target, and the unauthorized result [2].

Several attempts to modify or expand on Howard and Longstaff's taxonomy have been made. Maria Kjaerland proposed a taxonomy that included the source and target sectors along with the method of operations and the impact to the target [3]. Clive Blackwell focused on the defensive posture of the victim of an attack. Where Howard and Longstaff focused on the objectives of the attacker, Blackwell attempts to understand the ultimate effect on the target [4].

Other taxonomies include the four dimensions of an attack defined by Hansman and Hunt [5] and the AVOIDIT taxonomy [6]. Each of these taxonomies provides a valuable methodology for looking at an attack. However, none of these taxonomies considers the unique characteristics of CPS. Existing taxonomies do not provide a comprehensive method for analyzing an incident in the context of the market sectors that are impacted. They also do not provide a means of analyzing incidents in the view of their impact on the physical world.

Cyber-Physical Systems

The first challenge in classifying incidents in CPS is that there is no clear definition of what a CPS is. We found that in the context of security, the definition of CPS has generally been limited to ICS and SCADA systems [7]. This view is narrowly focused and omits other system types that extend beyond critical infrastructure. A broader definition would be any system that combines computers, networks, and physical interactions [8]. CPS has also been defined as systems that bridge the world of computing and communication with the physical world [9]. A more accurate definition, and the one that we believe to be the most fitting for this framework, is that a CPS is a system that embeds the capabilities of cyber systems in the physical world. This type of system would operate on humans, infrastructure, or platforms to modify interactions with the physical world [10]. The term "cyber-physical" itself is intended to denote the interactions between computer systems and the real world [11].

Security should be of greater concern to this larger scope of cyber-physical systems. For instance, the health care industry should be more concerned with the rampant malware on medical equipment [12] or the ability for non-medical personnel (or attackers) to access or change information on implanted medical devices [13]. There are also vulnerabilities within the automotive industry that could be the source of incidents in the future [14,15].

Just as there are many definitions of what a CPS is, there is also confusion in how to classify cyber-attacks on these systems. There are two basic approaches to classifying incidents. The first approach focuses on the technology that is compromised in an incident. The second approach focuses on the application that is involved. Our taxonomy is applications-focused. In CPS, an incident tends to be more focused on the application of the system rather than which technologies are being utilized. The value of assets and mechanisms designed to protect them also tend to be application specific. Our classification system includes a variety of categories to describe an incident but is primarily focused on the market sector of the entity where the incident occurred.

CPS Market Sectors

There are many ways to classify the market sector in which a CPS functions. In developing the list below, we combined multiple approaches. We considered government sources, lists created by other researchers, our own evolving list, and, as a cross-check, the input of a large focus group.

The North American Industry Classification System [16] is a useful starting place; however, this classification system was developed in the 1930s for use by the US government [17]. Others have included short lists of areas where CPS might be used [8, 10]. What is needed is a comprehensive list of market sectors where CPS is used. With this goal in mind, we present the following list of market sectors that currently utilize CPS in their operations. This list was developed through several iterations of looking at industries and how they might be using CPS. We then invited a group of senior students studying Information Assurance and Security to develop their own list without our input. Finally, the results of these exercises were integrated to form the list presented in Table 1.

Table 1. Market sectors utilizing cyber-physical systems

Market Sectors
Utilities
Industrial Process Control
Health Care
Transportation
Aerospace
Military
Consumer Electronics
Facilities Infrastructure
Agriculture
Physical Access Control
Communications
Construction
Media Creation and Distribution

Incident Taxonomy

With the limitations of the existing taxonomies in mind, we have developed this new taxonomy. This taxonomy expands on the work that has already been done and addresses the key missing features of the alternative choices.

Incidents are classified based on several factors. These factors are market sector, source, means, impact, and victim. We have already described how we account for the market sector. The impact classification accounts for the physical aspects of an incident along with the information aspects. We also allow for the possibility that an incident can be classified in multiple categories. We will briefly describe each category then provide the list of possible classifications within the category.

Source Type

The source type describes the entity where an incident was initiated. The list in Table 2 attempts to comprehensively address the spectrum of possible sources. It should also be noted that an incident may include a single source or it may have multiple sources. A non-profit organization classification is assigned when an incident originates with a recognized NPO. The identified group classification is used in the case of a group that is not officially organized and has no legal recognition such as anonymous. The unknown classification is used when the source of an incident has not been identified.

Table 2. Incident sources

Source Type
Commercial
Government
Educational
Non-Profit Organization
Individual
Identified Group
Unknown

Means

The means of an incident denote how the incident occurred. This could be the methods used if the incident was a deliberate attack or the things that went wrong in the case of an unintentional failure. Note that a single incident can involve multiple means. While almost any incident could be classified as a misuse of resources, this classification is reserved for those cases where an authorized user of the system used it in a manner that was not authorized or intended.

Table. Incident means

Means
Misuse of Resources
User-level Resource Compromise
Root-level Resource Compromise
Social Engineering
Virus
Web-site Compromise
Trojan
Worm
Recon
Denial of Service
Other System Failure

Impact

The impact of an incident describes the effect of the incident. The description of the impact needs to address all the affected entities; these include the computer system, the physical system that the CPS interacts with, and the broader impact on the organization and community too. There are both direct and indirect impacts of any incident.

The direct impacts of an incident are typically those that are easily seen. These are the impacts that may be discovered immediately or within a short time-frame. The classifications for direct impact are presented in Table 4.

Table 4. Direct impacts

Direct Impact
Service Disruption
Information Distortion
Physical Destruction
Environmental Destruction
Information Destruction
Information Disclosure
Death/Serious Injury
Unknown

Indirect or intangible impacts are sometimes harder to quantify. The indirect impacts may not be seen for several years following an incident. In many cases, the indirect impacts are more costly than the direct impacts. When these indirect impacts are combined, the costs of an incident increase significantly. The indirect impacts are listed in Table 5.

Table 5. Indirect impact

Indirect Impact
Loss of Reputation
Loss of Trust
Lost Business
Political Repercussions
Public Response

When determining the full impact of an incident, it is necessary to account for the level of severity of the impact. The severity is a modifier to the impact as already defined. We have modified a typical low, medium, high severity scale to account for the unique nature of CPS. This scale is shown in Table 6.

Table 6. Impact severity

Severity of Impact
Inconvenience
Secondary Operations Degraded
Secondary Operations Halted
Primary Operations Degraded
Primary Operations Halted

Other factors in the impact of an incident include how long it takes for the impacts to be recognized, the time to recover from an incident, and the cost of the incident.

The immediacy of an impact describes how long it takes after an incident for the impact to be recognized. This could be seconds, minutes, hours, days, or even longer. This is not necessarily an increasing or decreasing scale of impact. The immediacy is a modifier that allows us to understand the context of the impact better.

The time it takes to recover from an incident is another indication of the impact of the incident. The longer it takes to recover from an incident, the greater the impact is.

A component of the impact of an incident is also the cost of the incident to the victim. This cost could be hard costs such as the cost to repair the system, or soft costs like lost revenues due to system down time.

Victim

The victim describes the entity where an incident took place. We will classify the victim in two ways. First, we will identify the victim type. The types are the same as for the source and the same rules apply.

Table 7. Victim type

Victim Type
Commercial
Government
Educational
Non-Profit Organization
Individual
Identified Group
Unknown

We will also describe the victim of an incident based on our classification of CPS market sectors. We have developed a tree hierarchy for each market sector that shows how the sector breaks down into various industries and activities. Although the classification scheme shown is strictly hierarchical, we recognize that some incidents can fall within multiple sectors. Therefore, this strict hierarchy is not imposed on the classification of incidents. It is possible for a victim to be classified under multiple market sectors. This provides further flexibility and utility in the system as incidents may be classified and found in the multiple contexts where they are important.

Table 8. Victim market sectors

Victim Market Sectors
Utilities
Industrial Process Control
Health Care
Transportation
Aerospace
Military
Consumer Electronics
Facilities Infrastructure
Agriculture
Physical Access Control
Communications
Construction
Entertainment Media Creation and Distribution

Utilizing this taxonomy allows for analysis of incidents based on the vertical market sector along with the impact of an incident and other factors that are overlooked in many incident taxonomies. The complete taxonomy can be seen in Figure 1.

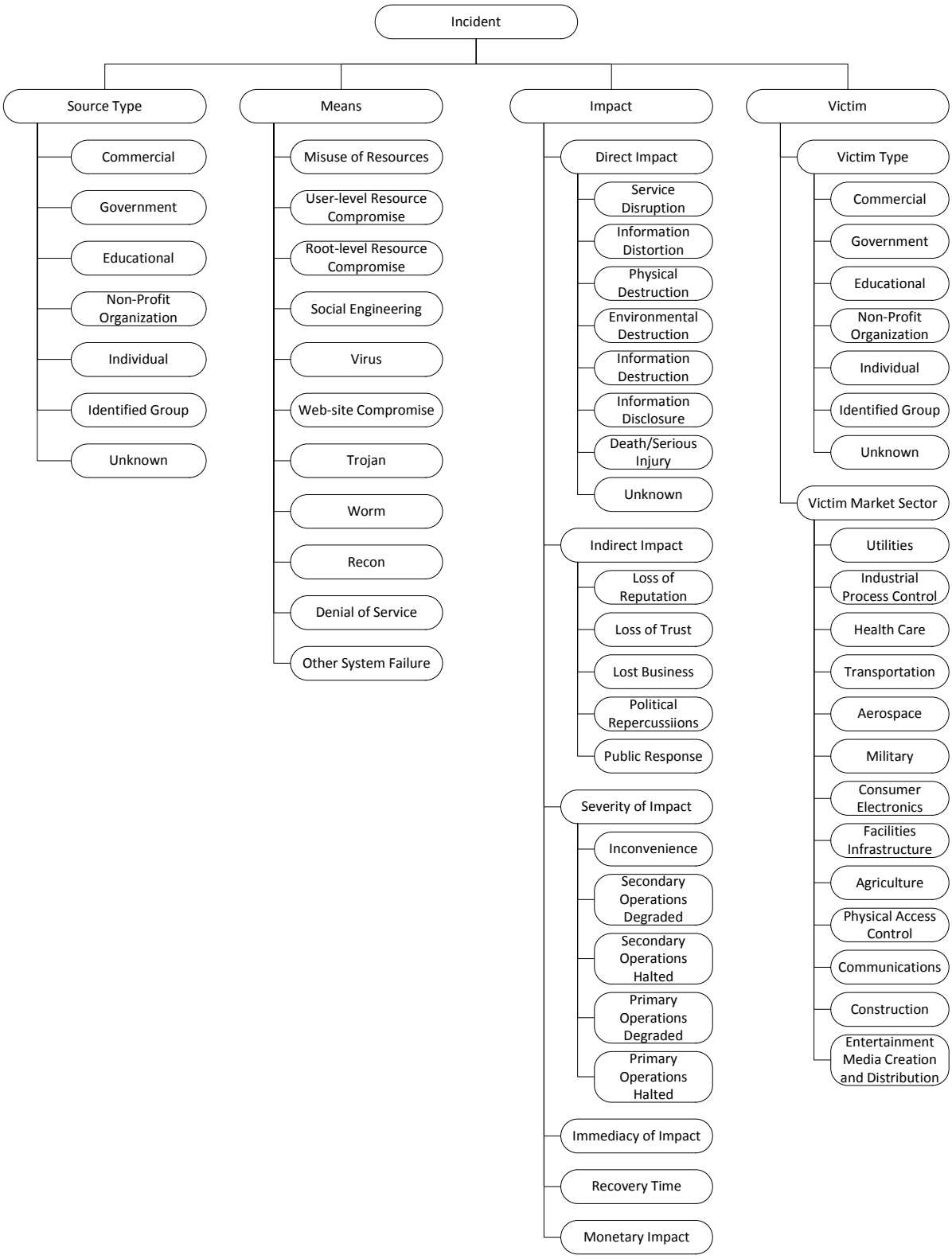

Figure 1. CPS incident taxonomy

Incident Classification Examples

We present some experimental scenarios of incidents involving CPS and some real examples of these types of incidents and demonstrate how they would be classified within our system.

Several recent incidents and security failure demonstrations have shown how systems can be compromised through cyber-attacks. We will present two examples and show how they can be classified with this incident classification system. We will then present several other types of incidents, both actual and theoretical, and show how these can also be classified in this system.

In 2010, researchers from the University of South Carolina and Rutgers University demonstrated several vulnerabilities within vehicle tire pressure sensors. These researchers were able to track a vehicle using the unique identifiers broadcast by the tire pressure sensors as well as spoof low pressure warning signals to the vehicle [20]. *Source Type*: educational; *Means*: misuse of resources, recon; *Direct Impact*: service disruption, information distortion, information disclosure; *Indirect Impact*: none at this time, but a real life attack could result in loss of reputation, loss of trust, political repercussions, and public response; *Severity of Impact*: inconvenience; *Victim Type*: individual; *Victim Market Sector*: transportation.

Researchers from the University of Washington and the University of California San Diego were able to demonstrate the capability of using the cellular network to attack vehicle telematics systems such as GM's OnStar or Ford's Sync [14]. *Source Type*: educational; *Means*: misuse of resources; *Direct Impact*: service disruption, information distortion; *Indirect impact*: loss of reputation, loss of trust, lost business, political repercussions, public response; *Impact Severity*: secondary operations degraded, primary operations degraded, primary operations halted; *Victim Type*: individual; *Victim Market Sector*: transportation.

Beth Israel Deaconess Medical Center in Boston has 664 pieces of medical equipment that run on older versions of the Microsoft Windows Operating System. The manufacturers of this equipment will not allow the hospital to modify the systems even to install anti-virus software due to certification requirements. This equipment is often infected with malware, and one or two devices have to be taken out of service each week to be cleaned [12]. *Source Type:* unknown; *Means:* misuse of resources, virus; *Direct Impact:* service disruption, death/serious injury; *Indirect Impact*: loss of reputation, loss of trust, public response; *Severity of Impact*: primary operations degraded; *Victim Type*: non-profit organization; *Victim Market Sector:* health care.

In June 1999, 237,000 gallons of gasoline leaked from a 16" pipeline into a creek that flowed through Whatcom Falls Park in Bellingham, Washington. About 1 1/2 hours after the rupture, the gasoline ignited and burned approximately 1 1/2 miles along the creek causing 3 deaths and 8 documented injuries. The pipeline failure was exacerbated by control systems not able to perform control and monitoring functions. The National Transportation Safety Board report issued October 2002 cited one of the five key causes of the accident was the Olympic Pipe Line Company's practice of performing database development work on the SCADA system while the system was being used to operate the pipeline [21]. *Source Type:* user; *Means:* misuse of resources; *Direct Impact:* service disruption, physical destruction, environmental destruction, death/serious injury; *Indirect Impact*: loss of reputation, lost

business, political repercussions, public response; *Impact Severity*: primary operations halted *Victim Type*: commercial; *Victim Market Sector:* utilities.

This example shows that an attack can be multi-classified. In March 1997, one hacker penetrated and disabled a telephone company computer that serviced Worcester Airport in Massachusetts. As a result, the telephone service to the Federal Aviation Administration control tower, the airport fire department, airport security, the weather service and various private airfreight companies were cut off for six hours. Later in the day, the juvenile disabled another telephone company computer, this time causing an outage in the Rutland area. The outage caused financial losses and threatened public health and public safety [22]. *Source Type*: individual; *Direct Impact*: service disruption; *Indirect Impact*: public response; *Impact Severity*: secondary operations degraded, primary operations degraded; *Victim Type*: government, commercial; *Victim Market Sector*: transportation, communications, physical access control.

In February 2013, the Emergency Alert System for television station KRTV in Montana broadcast a warning that "The bodies of the dead are rising from their graves and are attacking the living." [23]. *Source Type*: unknown; *Means*: user-level resource compromise; *Direct Impact*: service disruption, information distortion; *Indirect Impact*: loss of trust; *Impact Severity*: inconvenience; *Victim Type*: commercial; *Victim Market Sector*: communications.

In January 2003, the SQL Slammer worm infected the Davis-Besse nuclear power plant in Ohio, USA. As a result of the worm's activity, the plant's safety parameter display system and plant process computer were disabled for several hours [24]. *Source Type*: unknown; *Means*: worm; *Direct Impact*: service disruption, information distortion; *Indirect Impact*: loss of trust, political repercussions; *Impact Severity*: secondary operations halted *Victim Type*: commercial; *Victim Market Sector*: utilities.

In June 2010, it was discovered that a worm dubbed Stuxnet had struck the Iranian nuclear facility at Natanz. Stuxnet used four "zero-day vulnerabilities" (vulnerabilities previously unknown, so there has been no time to develop and distribute patches). The worm employs Siemens' default passwords to access Windows operating systems that run WinCC and PCS7 programs. The worm would identify and attack frequency-converter drives made by Fararo Paya in Iran and Vacon in Finland. These drives were used to power centrifuges used in the concentration of the uranium-235 isotope. Stuxnet altered the frequency of the electrical current to the drives causing them to switch between high and low speeds for which they were not designed. This switching caused the centrifuges to fail at a higher than normal rate [25]. *Source Type*: government; *Means*: worm; *Direct Impact*: service disruption, physical destruction; *Indirect Impact*: political repercussions; *Impact Severity*: primary operations degraded; *Victim Type*: government; *Market Sector*: utilities, military.

In a similar case to the SQLSlammer worm, also in 2003, a computer virus named Sobig was reported to have shut down train signaling systems in Florida. The virus was reported to have been one of the fastest spreading e-mail attachment viruses at the time. It shut down the signaling, dispatching and other systems at CSX Corporation; one of the largest transportation suppliers in the U.S. While there were no major incidents caused by this case,

trains were delayed [26]. *Source Type*: unknown; *Means*: virus; *Direct Impact*: service disruption, information distortion; *Indirect Impact*: lost business; *Impact Severity*: primary operations degraded; *Victim Type*: commercial; *Victim Market Sector*: transportation.

In Maroochy Shire, Queensland, Australia, in 2000 a disgruntled ex-employee hacked into a water control system and flooded the grounds of a hotel and a nearby river with a million liters of sewage. The Maroochy Shire attack was not one attack but a whole series of attacks over a prolonged period [27]. *Source Type*: individual; *Means*: user-level resource compromise; *Direct Impact*: service disruption, information distortion, environmental destruction; *Indirect Impact*: loss of trust, political repercussions, public response ;*Impact Severity*: primary operations degraded; *Victim Type*: government *Victim Market Sector*: utilities.

In 1999, hackers broke into Gazprom, a gas company in Russia. The attack was collaborated with a Gazprom insider (disgruntled employee). The hackers were said to have used a trojan horse to gain control of the central switchboard, which controls gas flow in pipelines [24]. *Source Type*: unknown; *Means*: user-level resource compromise, trojan; *Direct Impact*: service disruption, physical destruction; *Indirect Impact*: loss of reputation, lost business, political repercussions; *Impact Severity*: primary operations degraded; *Victim Type*: commercial; *Victim Market Sector*: utilities.

Cyber-Physical Systems Incident Database

Just as there are multiple incident taxonomies available, there are also different incident databases available. The Repository of Industrial Security Incidents (RISI), available at http://www.securityincdents.net, is an industry focused database of incidents. This database costs thousands of dollars per year for access and does not factor utilizations of CPS outside of industrial control systems. For example, there is no consideration for the communications or health care industries within RISI. The US-CERT database, available at http://www.us-cert.gov, is another example. This database focuses on vulnerabilities rather than incidents, has no consideration for CPS, is US-focused, considers a limited range of sectors, and is not updated for more recent developments in platforms.

The framework that has been presented has been used to develop an incident database. This database is designed to be a repository of incidents along with their classifications. Information about incidents is gathered from currently available sources and compiled into a single repository. This database may be used for academic research into CPS incidents and is freely available to researchers in this area. The database is hosted by the Brigham Young University Cyber Security Research Lab and may be accessed at http://cpsid.et.byu.edu by the time of this publication.

Unfortunately, due to the malicious intent of a relative few, it is necessary to perform some sanitization of the public incident database to help minimize the risk of misuse. Two levels of protection are implemented in the online database. The first is the sanitization of records; this removes sensitive information and details from recorded incidents that may be misused. The second level of protection we shall implement is access control and a requirement to register for complete unsanitized access. Users will be required to register with a valid

institutional, organizational, government or recognized corporate domain. They will then be granted access subject to a basic verification of their request.

Future Work

The initial goal of this work was to develop the taxonomy, complete the CPSID, and make it publicly available. No attempt has been made to analyze the contents of the database. A methodology for analyzing the contents of the database needs to be developed. This analysis should focus on identifying trends, commonalities, and differences in these incidents. This analysis should provide understanding into how CPS incidents happen and how they can be prevented.

Understanding that it is impossible to prevent all possible incidents, steps need to be taken to minimize the occurrence of incidents and the impact these incidents have. The analysis of incidents included in this database should be used to develop these methodologies for minimizing both the occurrence and impact of CPS incidents. Above all, these methodologies should focus on protecting the people and the environment that surround these systems.

Conclusion

We have presented a detailed yet highly adaptable CPS security incident taxonomy. The classification system allows for precise and flexible classification of security incidents. As the system is adopted and the database is populated it allows for detailed analysis of the types, frequency and impact of incidents, which in turn enables a directed approach to mitigating the consequences of incidents and will also lead to improved risk management and design approaches for future systems.

A significant benefit of the approach is that each incident is recorded with significant contextual information. A malicious break-in that causes inconvenience in an entertainment context is of less concern than an accidental error in health care leading to potential loss of life, although they could both employ the same means in the attack execution (for example, the SQL slammer worm). Permitting cross-classification also allows related incidents to be identified in different areas.

The field of CPS security is young but growing very rapidly. We anticipate future research and development of the system in several possible directions. Some possible future developments include combining the information with comprehensive design approaches for CPS, tracking and updating incident records as further information emerges and analyzing the types and frequency of incident occurrences. Further detail of the technologies used in the incidents could also be added as supplementary information.

The openness and cost (free) of the database is intended to encourage adoption and rapid growth.

References

[1] Miller, B & Rowe, D. (2012). A Survey of SCADA and Critical Infrastructure Incidents. *Proceedings of the 1st Annual Conference on Research in Information Technology*, 51-56.

[2] Howard, J. D., & Longstaff, T. A. (1998, October). *A Common Language for Computer Security Incidents*. Sandia Report # SAND98-8667. Retrieved from http://prod.sandia.gov/techlib/access-control.cgi/1998/988667.pdf
[3] Kjaerland, M. (2006, October). A Taxonomy and Comparison of Computer Security Incidents from the Commercial and Government Sectors. *Computer Security*, *25*(7), 522-538.
[4] Blackwell, C. (2010). A Security Ontology for Incident Analysis. *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, 1.
[5] Hansman, S., & Hunt, R. (2005). A Taxonomy of Network and Computer Attacks. *Compuer. Security*, *24*(1), 31-43.
[6] Simmons, C., Dasgupta, S. S., & Wu, Q. (2009). *AVOIDIT: A Cyber Attack Taxonomy*. University of Memphis, Technical Report # CS-09-003.
[7] Neuman, C. (2009). Challenges in Security for Cyber-Physical Systems. *Workshop on Future Directins in Cyber-Physical Sytsem Security*.
[8] Broman, D., Lee, E. A., Torngren,M. & Sunder, S. S. (2012). Cyber-Physical Systems —A Concept Map. Retrieved from http://cyberphysicalsystems.org/
[9] Rajkumar, R., Lee, I., Sha, L. & Stankovic, J. (2010). Cyber-Physical Systems. *Proceedings of the 47th Design Automation Conference*, 731.
[10] Poovendran, R. (2010, August). Cyber–Physical Systems: Close Encounters between Two Parallel Worlds. *Proceedings of the IEEE*, *98*(8), 1363-1366.
[11] Helps, R. & Mensah, F. (2012). Comprehensive Design of Cyber Physical Systems. *Proceedings of the 13th Annual Conference on Information Technology Education (SIGITE '12)*, 233-238.
[12] Talbot, D. (2012, October 17). Computer Viruses Are "Rampant" on Medical Devices in Hospitals. *Technology Review*. Retrieved from http://www.technology review.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/
[13] Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S, S., Defend, B., Morgan, W., Fu, K., Kohno, T., &Maisel, W. H. (2008, Spring). Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, 129-142.
[14] Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., & Kohno, T. (2011). Comprehensive Experimental Analyses of Automotive Attack Surfaces. *Proceedings of the 20th USENIX conference on Security*, 6.
[15] Brooks, R. R., Sander, S., Deng, J., &Taiber, J. (2008). Automotive System Security. *Proceedings of the 4th Annual Workshop on Cyber Security and Informaiton Intelligence Research Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead*, 1.
[16] U. C. B. S. P. Staff (2012). *US Census Bureau Site North American Industry Classification System Main Page*. Retrieved from http://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012
[17] Dalziel, M. (2007, December). A Systems-Based Approach to Industry Classification. *Research Policy*, *36*(10), 1559-1574.

[18] Weaver, N., Paxson, V., Staniford, S., & Cunningham, R. (2003). A Taxonomy of Computer Worms. *Proceedings of the 2003 ACM Workshop on Rapid Malcode*, 11.
[19] Mirkovic, J., & Reiher, P. (2004, April). A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39.
[20] Rouf, I., Miller, R., Mustafa, H., Taylor, T., Oh, S., Xu, W., Grutese, M., Trappe, W., & Seskar, I. (2010). Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study. *Proceedings of the 19th USENIX Security Symposium*, *39*(4), 11-13.
[21] Tsang, R. (2010). Cyberthreats, Vulnerabilities and Attacks on SCADA Networks. Goldman School of Public Policy. University of California: Berkeley, CA.
[22] Denning, D. E. (2004). Cyberterrorism: The Logic Bomb versus the Truck Bomb - Centre for World Dialogue. *Global Dialogue*, *2*(4). Retrieved from http://www.worlddialogue.org/content.php?id=111
[23] Bhasin, K. (2013, February 11). Montana TV Station Apologizes for Emergency Broadcast about Zombie Apocalypse. *Business Insider*. Retrieved from http://www.businessinsider.com/krtv-zombie-apocalypse-alert-2013-2
[24] Veerasamy,N., Grobler, M., & Von Solms, B. (2006, June). Building an Ontology for Cyberterrorism. *Proceedings of the 5th European Conference on Information Warfare and Security: National Defence College, Helsinki, Finland*.
[25] Farwell, J. P. & Rohozinski, R. (2011, February). Stuxnet and the Future of Cyber War. *Survival*, *53*(1), 23-40.
[26] Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012, March). SCADA Security in the Light of Cyber-Warfare. *Computer Security*, *31*(4), 436-418.
[27] Mustard, S. (2005). Security of Distributed Control Systems: The Concern Increases. *Computing & Control Engineering Journal*, *16*(6), 19-25.

Biographies

WILLIAM B. MILLER is currently a graduate student in the Information Technology Department at Brigham Young University. His research interests include information assurance and security and cyber-physical systems. He has over 15 years of experience in systems administration. Mr. Miller may be reached at Bill_Miller@byu.edu.

DALE C. ROWE is an assistant professor of Information Technology at Brigham Young University and Director of the Cyber Security Research Laboratory. He maintains a variety of security certifications including a CISSP. Dr. Rowe's scholarly interests include anything security related and he enjoys keeping his technical skills up to date. In 2011, he created and maintains a student Red Team which frequently conducts penetration tests as a service to the local community. In the past 3 years, he has mentored 4 cyber defense (CCDC) student teams who have received twice 3rd place, 2nd place and 1st place in regional contests. Prior to joining BYU in 2010, he worked as a systems security architect in the aerospace industry. Dr. Rowe may be reached at dale_rowe@byu.edu.

C. RICHARD G. HELPS is currently an associate professor of Information Technology at Brigham Young University. He is a member of ACM (SIGITE), IEEE and an ABET commissioner. His primary scholarly interests are in cyber-physical or embedded systems. Designing these systems incorporates interesting system-design principles and overlaps into related interest areas, such as human-computer interaction and systems integration. He also has interests in technology curricula and course design to meet the needs of ever-changing technical university courses. This has led to a long-term involvement in accreditation and in national IT education entities. Dr. Helps may be reached at Richard_Helps@byu.edu.

ROSS N. WOODSIDE is an undergraduate student in the Information Technology Department at Brigham Young University where he has worked with the Cyber Security Research Lab since March of 2013. His major interests are in penetration testing, digital forensics, and information assurance. He plans on graduating in April of 2015 after completing an internship with Goldman Sachs over the summer in their Tech Risk Department.