

ARTIFICIALLY INTELLIGENT INDUSTRIAL CONTROLLERS

By

Joseph Wayne Davis

A Capstone Project Submitted to the Faculty of

Utica College

August 2015

In Partial Fulfillment of the Requirements for the Degree of

Master of Science in

Cybersecurity

© Copyright 2015 by Joseph Wayne Davis

All Rights Reserved

Abstract

Control of and access to critical industrial controllers requires updated security. Artificial Intelligence may prove valuable by increasing resiliency and reducing the vulnerabilities to such systems. Improving security deficiencies relevant to the control of these systems is dependent on future development of cyber-physical tools and analysis methodology. Programmable industrial controllers are targets in the cyber domain. Code designs are a warfare tactic and nation-states execute them against one another. In its current format, legislation for provisional oversight does not effectively protect systems that maintain critical infrastructure. Present difficulties exist in these systems due to implementing added connectivity attributes as well as the vulnerabilities due to the system interdependency of Supervisory Control and Data Acquisition Systems (SCADA). Present day programmable logic controllers have no inherent ability to mitigate, identify, or notify industrial technicians about malicious activity. Many industrial control engineers generally have minimal knowledge of cybersecurity. Information technology technicians do not understand the fragile and complex nature of industrial control systems. Further, mainstream dependence on the business technique of risk management reduces the focus and evolution of alternative cybersecurity techniques. Adoption of Artificially Intelligent Industrial Controllers within unconscious expert databases has the prospect to improve security for Industrial Control Systems and deliver Resilient Control Systems through designs including perception, fusion, and decision-making abilities. Implementing improved static attributes for these systems should include active defense constructs to garner optimum benefit. Controlled test environments to prove the efficacy of proposed research and development are necessary.

Keywords: Cybersecurity, Professor Christopher Riddell, Artificial Intelligence, Industrial Controller, PLC, Advanced Persistent Threat, Cyberweapons, CIKR, Resilient Control Systems

Acknowledgments

I owe a debt of gratitude to many for the years of positive encouragement, wisdom, grace, love, and blessings bestowed upon me throughout this journey. Primarily I must extend humble and contrite thanks to one of the strongest women I have ever met, my wife Shelby. Expressing her constant reinforcement and understanding is not fully collected in words. To you I dedicate this work's representation of the completion of this degree and journey. You have always seen each task through with me and for that- I love you. To my children and the many other family members who understood why I could not attend gatherings or activities due to school. To all the Utica staff who devoted their time and energy to deliver the knowledge of cybersecurity and other curriculum I extend my thanks. Those who teach truly are one of the world's greatest gifts. To Professor Christopher Riddell who took the time to work with me in a out of class aspect which I think delivered an exceptionally improved product overall. Thanks to all who took time to review and assist in the editing process; Aris Theocris, Robert M. Lee, and J. Lopez. I dedicate the topic and understanding this paper delivers about industrial control systems to Arthur Zatarain. Thank you for taking the time to be my second chair and devoting the time to review this work from your level of technical expertise. I dedicate the technical aspect of this work to the drive and diligent integrity bestowed by Randall K. Nichols (*aka The Dragon*). Few people retain a level of commitment and true desire to help a person succeed. Thank you sir for being a true mentor, friend, and a wealth of wisdom. I dedicate the potential that this work may bestow to the many others who practice in the field and who took time to speak with me or allow me access to resources on the topic-thanks.

Table of Contents

Abstract	i
Acknowledgments.....	ii
Artificially Intelligent Industrial Controllers	1
Deficiencies in the Evidence	6
Literature Review.....	6
IC Security Deficiency	6
Absence of law.	6
Defensive posture.	8
Active defense	9
Attack surface.....	9
Supervisory control and data acquisition scenarios.....	11
XP machines not retired.	13
Infrastructure catastrophes.....	15
Potential impact.	16
Mitigating IC Vulnerabilities	18
Service vs. security.....	18
Corporate vs. industry.....	20
Typical security technology.....	22
ICS configuration weaknesses.....	24
ICS network weaknesses.	25
Resilient Systems	26
AI obstacle.....	26
Resilient control systems.....	27
Cyber awareness.....	29
Data fusion.....	30
Simplifying intelligible design.....	31
Discussion of Findings.....	33
Governmental Incompetence.....	33
Growing Target Topology.....	35
Conditioned for Exploit.....	36
Failure to Upgrade.....	38
Minimal Risk Perspective	38
Prevention Not the Focus	39
ICS Security Deficiency.....	40
Need for Advanced Security in IC	42
Evaluating AI	42
The Reality of Resiliency	43
Applying Data Fusion to CI	44
Merging CI and Simplified Intelligible Design	4544
How AI Mitigates.....	45
How AI Improves IC.....	4645
Critical Findings.....	46
Future Research and Recommendations.....	47
Redirected Mitigation.....	47
Conceiving AIIC	48

Application of AIIC	<u>4948</u>
Questions for Future Research	49
References	50
Appendices.....	67
Appendix A- Hacking or Disruption to SCADA	67
Appendix B- List of Abbreviations.....	68

List of Illustrative Materials

Figure 1. IA defense in depth strategy 3

Figure 2. ICS network diagram 4

Figure 3. Active Cyber Defense Cycle 9

Figure 4. ICS-CERT response analysis for 1st half of 2013 10

Figure 5. Windows 7 Requirements 14

Figure 6. SCADA interdependencies 18

Figure 7. Basic control loop recreated 20

Figure 8. Job Qualification 21

Table 1. Challenges for Control Systems 21

Table 2. Basis for Policy 29

Table 3. Principles for Critical Infrastructure Security..... 31

Table 4. Tough Questions for Cybersecurity 34

Figure 9. Davis Cyberattack Loss Equation 35

Figure 10. Effects of Cyberattack Loss 36

Figure 11. Electric Turbine Cyberattack..... 37

Artificially Intelligent Industrial Controllers

The purpose of this research was to propose increased role for Artificial Intelligence (AI) for adaptive measures in cybersecurity for Industrial Controllers (IC) to provide Resilient Control Systems (RCS) and improve cybersecurity for such devices. Control of and access to critical industrial controllers requires updated security. AI may prove valuable by increasing resiliency and reducing the vulnerabilities to such systems. The proposed research improves upon the defense-in-depth strategy with an added layer to mitigate current security vulnerabilities. Key questions include: What indicates a need for advanced security in industrial controllers in current systems? How can AI mitigate vulnerabilities and threat levels to Industrial Control Systems (ICS) and critical infrastructure? How will AI improve IC to introduce RCS?

Malicious computer code, first identified in 2010, targets IC's. Stuxnet's ability is a model of "malware" capable of infiltration and destruction of specific process control hardware (Nakashima & Warrick, 2012). Code designed as a warfare tactic and executed by a nation-state lead to the term "cyberweapon." A succinct description of cyber weapon are cyber means a conflict intended to cause injury or death of people or damage to, or destruction of objects (International Group of Experts, 2013). A substantial issue is increasing terrorist events and malevolent code targeting Critical Infrastructure and Key Resources (CIKR). Attacks designed to damage or disrupt infrastructure target ICS (Bologna, Fasani, & Martellini, 2013).

Stuxnet demonstrated hardware destruction within infrastructure equipment through logical means. The advanced persistent threat (APT) specifically targeted Siemens' programmable logic controllers (Nakashima & Warrick, 2012). The exploit indicated that cyberweapons are possible and that IC's are vulnerable to computer exploits. The modular development, compartmentalized design, and short list testing with *false flag* attribution of the

code demonstrated sophistication. Use of stolen digital signatures from Realtek and JMicron gave Stuxnet its stealth (Matrosov, Rodionov, Harley, & Malcho, 2011). Further, Stuxnet could adjust logic within IC's. Once the target components were found, their standard operating parameters were changed by Stuxnet. Of three attack modules, two were specifically associated with modifying IC's responsible for centrifuges in Iran's Natanz Uranium enrichment plant (Mueller & Yadegari, 2012). Stuxnet's programming included sensor control to hide parameters implemented by its operations. These parameters mean analyst did not see an incident. Technicians surveying operations saw only normal readings. The introduced parameters caused the centrifuges to run at low and high intervals over a period of time (Mueller & Yadegari, 2012). The resulting outcome is scuttled hardware.

Extensive installations of networked industrial controllers in diverse applications are in operation around the world. The wide use of IC's necessitates resilience of these systems (Bologna et al., 2013). Such systems identifiable as specific points of risk make up these networks (Shea, 2003). Disruption or destruction of IC's can present ramifications to health, safety, security, and economics (Bologna et al., 2013). The United States (U.S.) CIKR falls into this category (Shea, 2003).

Access restrictions are minimal. Therefore, unauthorized modification can occur within an ICS. Hackers can use remote access locations to breach firewalls and access Modbus devices. Achieving access to Modbus devices makes it possible to program control logic set points and manipulate operation of programmable logic controllers.

CIKR no longer preserves boundaries that restrict infiltration from external networking. Businesses now link CIKR to the Internet, compromising the ideal state for an Industrial Control Network (ICN) (Ferguson, 2012). Interlocking these networks with the Internet necessitates that

mainstream Information Technology (IT) adopt defense-in-depth protocols. Involving patch management, network segmentation, authentication, application control, event management, and intrusion management is an expectation in these systems (Ferguson, 2012). All are facets of the technology division of Information Assurance (IA). IA conjoins hardware and software with people, operations, and technology (The Information Assurance Directorate, 2002). ICS's are not atypical IT environments (Ferguson, 2012). Security postures associated with ICS's require better defensive metrics because they are involved in multi-tier frameworks. Their components can interface with enterprise networks (Ferguson, 2012). Available connections between enterprise and remote field locations validate IC security concerns. Figure 1 provides an example of the IA framework.



Figure 1. IA defense in depth strategy by Defense in Depth (The Information Assurance Directorate, 2002).

Organizations should; 1) expect attacks on these systems, 2) have tools to detect intrusion, and 3) procedures for incident response and recovery (The Information Assurance Directorate, 2002). A troubling feature of IC's is their physical link. This physical state connects to the virtual state presenting a keystone of ICS security. The entire façade is at risk of collapse without proper networking, operational procedure, and element segmentation (Ferguson, 2012).

Figure 2 presents the highly vulnerable and dependent nature of ICS's. These systems require air gaps. These gaps were dissolved by the necessity business perceives as important for real time access to data.

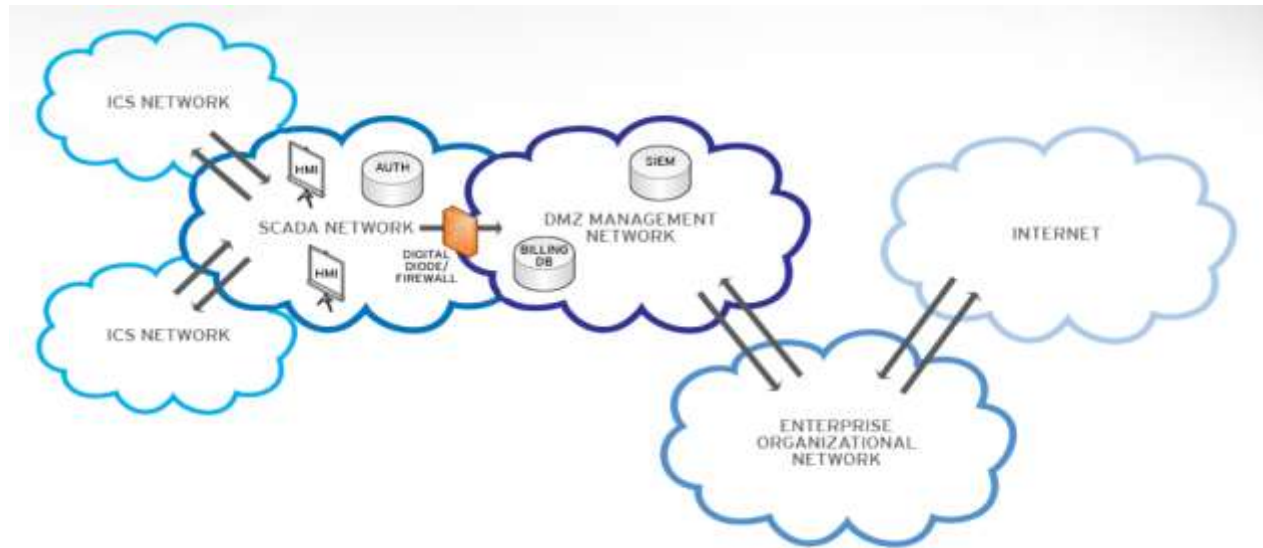


Figure 2. ICS network diagram by Toward a More Secure Posture for Industrial Control System Networks (Ferguson, 2012).

Although logical barriers linked with defense-in-depth configurations have become a part of national defense, they do not protect IC's. CIKR is dependent upon this IA metric to mitigate the potential for catastrophic events (Ferguson, 2012).

The basis for IA is risk management. This practice only indicates the potential for risk to CIKR environments. Contingency planning for such networks where a disaster will domino through CI does not have a physical mitigation technique or tool. Proof came in the form of Stuxnet illustrating the vulnerable condition of the mainstream network security architecture and its vulnerability regarding IC's. The cyberweapon highlighted the reality that many Supervisory Control and Data Acquisition (SCADA) sites contain points of failure (Matrosov, et. al., 2011). The push for synergy, efficiency, and real time data for marketing has attached the corporate networks to SCADA networks, thereby predisposing them to cyberattacks (Shea, 2003).

Business has fostered data linkage and networking within ICS's. Description of ICS architecture allows the reader to obtain a scope of these networks. For almost two decades the integrated data structure of Object Linking and Embedding for Process Control (OPC) has offered the connectivity and automation sought by industrial corporations (Spiegel, 2008). Next generation software named OPC Unified Architecture (OPC-UA) ushered in what business sought a backward compatible object-oriented and service-oriented design (Massaro, 2008). Interfaces contained in OPC-UA environments must afford secure access and immunity to malicious attacks, elevating security concerns (Paine, 2008). Malware, social engineering schemes, and advanced code similar to Stuxnet degrade the security applied to these networks.

Advancing AI could be the answer to increasing security for ICN's and IC's. Proposing systems secured by Artificial Security Intelligence (ASI) presents other challenges requiring examination. ASI can only become reality when a system entrusted with variables can accomplish autonomous decision-making skills in dynamic environments over extended periods (Horvitz, 1996). This condition has been the restricting dilemma present for conceptual ideas of AI. Moving such a technology forward has proved difficult in many aspects.

Adopting AI technology concepts validates the challenge confronting ICN's and technicians responsible for continual operation. This is true for an ICS indoctrinating ASI, a system that delivers utility throughout its lifetime and has no issue processing streams of events regularly is a normal expectation (Horvitz, 1996). The AI component also introduces the obstacle of teaching a program to learn. Systems cannot become artificially intelligent when they fail to discern what is adequate from inadequate (Horvitz, 1996).

Deficiencies in the Evidence

The perception of IT security is dissimilar at different levels in the corporate structure. Required awareness for IT security lacks communication and collaboration to improve current defenses (Mello, 2013b). Other than Stuxnet, no incident has raised concern. Corporate networks involved with CIKR secure their systems through standard IT provisions and attacks on IC's are new. Solutions for IC security concerns are possible through mainstream physical applications, risk assumption or transference. IT Security is taking a post-active position. Handling security problems happens per occurrence, becoming standard policy from that point (Mello, 2013b).

Improving computer operation through AI may not be feasible. AI does not apply the emotion, feeling, or instincts associated with humans. The current form of AI premised on logic causes shortcomings in decision-making (Chukwu, 2011). Moving past this obstacle requires research and development in AI. The potential to improve AI may be restricted. Limitations created by inconsistencies between multiple algorithms could lead to failures and overloads (Chukwu, 2011). The industrial systems addressed by this proposal cannot sustain shutdowns for testing. Introducing AI into ICS's would require controlled test environments. Each implementation would require its own test environment to ensure that execution would not result in damage. AI management of ICS's would require intelligent control strategies (Hayes-Roth, 1981).

Literature Review

IC Security Deficiency

Absence of law. Attempts at improving cyber legislation have been deficient. The absence of legislation causes issues for CIKR. The lack of production led to an executive order issued by the Obama Administration (Godreau, 2013). In February of 2013, the President (Executive Order [EO] 13636, 2013) signed EO 13636, the Preliminary Cybersecurity

Framework. This is a basis for cybersecurity infrastructure. It does not mandate how entities are required to secure their systems. Due to the absence of law, executives will view productivity over security because the cost of mitigation appears more than any perceived impact of cyberattack (Langner & Pederson, 2013). The EO explains the legislation as a public review and comment process conducted by the Cybersecurity Framework Director (EO 13636, 2013). Business governance steers the conduct of executives on issues of national security; cost is justified in terms of profit. Costs for security would be budgeted if fines or sanctions were the result.

The problems created by networked infrastructures are complex. Without law to dictate how to handle security in these environments, achieving forums for investigation and discussion will stall between government and industry (Godreau, 2013). Congressional cooperation on the issue is minimal. The last three Congresses proposed over one hundred bills though none became law (Fischer, 2013). Regulation is not the end resolution. Cybersecurity issues cannot be resolved with regulation alone (Godreau, 2013). The federal government defined 18 sectors within CIKR owned primarily by the private sector that require legislative action for increased security (Fischer, 2013). Bureaucracy prevents the increase. Extensive agreement exists that supplementary actions need to handle risks to CI caused by deficiencies in cybersecurity, however substantial disparity remains about any required additional federal regulation (Fischer, 2013, p. 13).

The inability of the government to enact legislation remands the problem to security practitioners. Several challenges exist that introduce tough questions for cybersecurity whereby a need is present to revise the National Infrastructure Protection Plan (NIPP). Questions related to responsibility, accountability, obligation, performance monitoring, provision of resources,

disaster liability, economic loss compensation, and societal responsibilities for increased security are not answerable by the current NIPP revision (Auerswald, et al., 2006). Practitioners use risk assessment for mitigation. Entities want manageable solutions to reduce threats (Honeywell, 2014). Risk assessment applications are helpful; however, they do not absolve the problem. Organizations that run ICS's admit to insufficient staffing for management of key elements (Honeywell, 2014). Though the federal government has indicated that these networks are vital, inaction leaves them self-reliant and susceptible to attack.

Defensive posture. Part of the problem stems from the rapid evolution of technology. Army General Keith Alexander mentions the need to protect networks including critical infrastructures (Roulo, 2014, p. 6). Another concern is NSA surveillance and its creation of public scrutiny. The division in agreement between the nation and its people on what is legal behavior in cyberspace slows progress (Roulo, 2014). The U.S. GAO implicates management issues as well that ultimately affect defense (US Government Accountability Office, 2011). Finding common ground is imperative to building better security concepts.

One other resounding issue for cybersecurity in general concerns a tunnel-vision approach. The intention depends on static processes and or tools meant to accomplish defensive postures for these architectures. In short, traditional defense is responsible for failure, due largely to the inability to provide traditional defense (Lee R. M., 2015). Cybersecurity requires processes that include dynamic attributes. Unfortunately, mainstream defensive techniques do not generally retain such properties. The ability to scrutinize and analyze a network at a granular level is not possible with just passive techniques (Lee R. M., 2015).

Active defense. The cybersecurity timeline contains valuable lessons learned that should be useful as hindsight. These findings show how important it is to apply security metrics through dynamic cyclic processes rather than relying on static or physical applications alone. Application of cybersecurity becomes more resilient when Tactics, Tools, and Procedure (TTP) couples with constant monitoring efforts. Monitoring efforts determine information about adversaries and their methods whereas simply using static tools to secure the network will eliminate this prospect (Bejtlich, 2014).

Active defense efforts are those such as the Active Cyber Defense Cycle (ACDC) proposed by Robert M. Lee. This dynamic cyclic process includes Asset Identification and Network Security Monitoring (NSM), Incident Response (IR), Threat Environment Manipulation (TEM) and Threat Intelligence Consumption (TIC). Figure 3 is an example of ACDC.



Figure 3. Active Cyber Defense Cycle by CYB 649: Advanced Topic in Cyber Operations. (Lee, R.M., 2015).

Attack surface. Losses due to cyberattacks against IC's are a function of achievable action and expected frequency (NSA, 2010). Attackers may not even require cyberweapons to infiltrate ICS's. A technique known as "spear phishing" uses deception to target specific individuals to achieve access to the target (Mello, 2013a). Surplus resellers present additional

vulnerabilities by remarketing unsanitized equipment pulled from factory floors and containing proprietary and or authentication information in the equipment’s memory (ICS-CERT, 2013).

Nefarious attackers could easily use this equipment to spearhead exploits.

Research performed via Shodan software revealed 95,000 devices that speak Modbus are reachable on the Internet (Higgins, 2013). The vulnerabilities of SCADA networks has risen more than 500% between 2010 and 2012 (Frei, 2013). The first half of 2013 showed 200 incidents requiring response by ICS-CERT across all sectors of CIKR as depicted in Figure 4 (ICS-CERT, 2013).

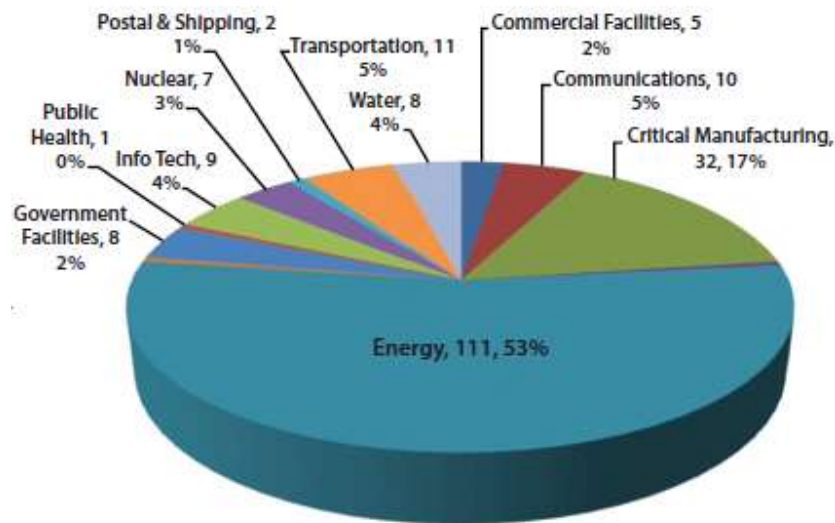


Figure 4. ICS-CERT response analysis for 1st half of 2013 by ICS-CERT Monitor (ICS-CERT, 2013).

The prospective threat sources expand the attack surface. Insiders, terrorists, activists, cybercriminals, nation-state sponsored attackers, and competitors can target ICS’s (NSA, 2010).

Note that these threats include both internal and external sources. Most of society uses computers though many of them have minimal technical skills or cyber awareness. Consider that some attacks may not be intentional and the level rises again. The Systems and Network Analysis Center for the NSA detailed a scenario about removable media spreading malware onto an ICS whereby the original plan for the infection was for another system (NSA, 2010).

Building a defensive position for an ICS is difficult. To begin a protective application on a standard network it must be mapped (Leverett, 2011). In respect of an ICS, commands used to map a network may create a hazard. For example, in one incident a plant experienced a loss of \$50,000 in integrated circuit wafers when a ping sweep caused the plant to hang (Stouffer, Falco, & Kent, 2006). Control system engineers will seek to keep these actions from happening though malicious players follow no restrictions (Leverett, 2011). With simple scans being so detrimental, ICS vulnerability is high and they have difficulty-achieving defense. The problem of implementing security measures reveals more of the attack surface.

Supervisory control and data acquisition scenarios. The vulnerabilities of SCADA are apparent within the present profile of cybersecurity. Modernized society is dependent on SCADA systems. SCADA systems influence the well-being of citizens and they remain targets for terrorism (Udassin, 2008). Another aspect to consider is the profile of the entity responsible for attacks on ICN's. Attacks presented by the proposed research derive from no ordinary hacker; well-funded and well-equipped control experts execute cyber assaults (Udassin, 2008). Illustrated in Appendix A is a list of twenty-nine events occurring between 1997 and 2009 related to SCADA hacks. Some of these events are purposed demonstrations; all are indicative of vulnerability inside ICS's. SCADA has three attack vectors- field attacks, corporate attacks, and physical attacks. In consideration of such environments and their previously mentioned states, vulnerability increases substantially.

Attacks on ICS's occur from the field, from corporate systems, and from physical attacks (Udassin, 2008). The proposed research emphasizes that virtual attacks multiply the cyber-attack vector rather than the physical one. Examining a physical field attack scenario emphasizes security issues of an ICN. Regulation of field devices takes place at the central hub where the

functions of an ICS's control servers reside (Udassin, 2008). The attribute of the field environment exhibits the initial issue. As in any line of defense, a broader defensive front weakens resistance.

Field workstations in unmanned areas allow infiltration into SCADA networks, making them challenging to secure and dependent upon physical security parameters such as fences and locks (Udassin, 2008). In very little time, a research team managed to determine vulnerability and execute an attack on a petroleum distribution entity in such a field location. Using a demo of the software running on the target system and the W32RTR.EXE process, arbitrary code exploited a heap based buffer overflow weakness. Buffer overflows dominate remote network vulnerabilities due to their provision of code injection and execution abilities (Cowan, Wagle, Pu, Beattie, & Walpole, 2000, p.1). The weakness uses a designer payload packet to exploit the system providing a remote shell with elevated privilege (Udassin, 2008).

This supports the information released by Italian researcher Luigi Auriemma who recorded thirty-four vulnerabilities associated with ICS's specifically related to heap overflows (Peterson, 2011).

Next is a review of an attack on a SCADA corporate network. Udassin (2008) indicates why corporate networks are easier targets in the following

- 1) They interface with the Internet;
- 2) Users in this environment are less educated about information security;
- 3) There are external machines hosted by the network.

The attack's objective is the firewall between the corporate network and the SCADA network.

The research team performed this attack using an out-of-the-box Proficy installation in conjunction with the Java remote method invocation protocol; this is required for a connection

between the Proficy web application and the user's browser (Udassin, 2008). The attack then uses intelligence-gathering tools to establish a connection.

An incorporated network sniffer aids the attack by disclosing a login packet where a clear-text username and encrypted data using Base 64 are exposed (Udassin, 2008). The password was located by using the intelligence in that packet which presented the encrypted Base 64 data. Another packet generated by the targeted user provided details. Through packet modification, file creation accomplished and gained the server's acceptance; an Active Server Page (ASP) file compilation opens a remote shell backdoor and bridge to the SCADA network (Udassin, 2008). The legacy code still used by SCADA systems ensures vulnerabilities are viable for future exploit (Peterson, 2011).

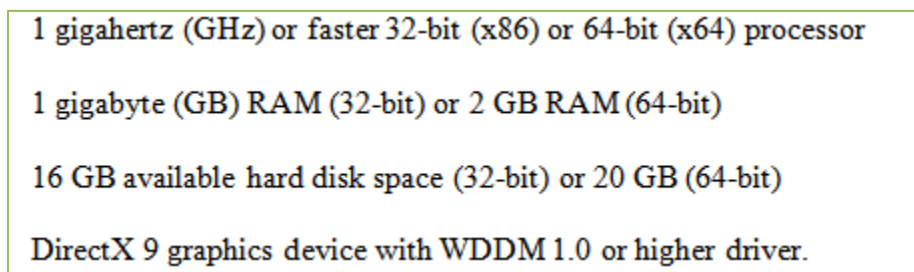
XP machines not retired. A large percentage of the population of computers still uses Windows XP. Microsoft ended support of XP on April 8, 2014 (BCS, 2013). Those machines running Windows XP in ICS's are susceptible to attacks. Approximately eighty percent of Britain's National Health Service is still using Windows XP (BCS, 2013). Computers still rely on Windows XP platforms for programming and monitoring of IC's currently (Zatarain, A. M., 2014). The changeover has been slow. Mission critical machines used for utilities are apart of this group (Shook, 2014). Older machines become obsolete because newer platforms require updated hardware (Clarke, 2013). Enterprise systems still using the old platform will have to be overhauled. Other areas of CIKR are migrating platforms but they are incomplete (Zatarain A. M., 2014).

One instance of the populace still widely using Windows XP is China. China is lagging behind in the migration to newer operating systems (OS). Part of the resistance is attributed to ideals that mitigation causes more potential for security threats (Ramzy, 2014). The analysis firm

StatCounter noted 49 percent of Chinese computers still use this Windows OS (Ramzy, 2014). Several reports of the five year old Conficker worm still affecting this region validates that many systems are using this OS (F-Secure, 2014).

Key problems are associated with Windows XP. This OS is difficult to repair once compromised. Two serious threats to Windows XP machines, *web-based attacks and Java-based attacks*, indicate prevention is advisable over seeking a cure (F-Secure, 2014). Another difficulty presents economic ramifications. “According to Bloomberg BusinessWeek, as many as 90% of all ATM machines are still running Windows XP” (F-Secure, 2014, p. 16). XP machines face a two-thirds increase in rate of infection after the final security patch (Keizer, 2014). Migrating the computers running this OS version will take time beyond the cut-off date. The percentages translate to approximately 488 million systems operating on XP as of February 2014 (Keizer, 2014).

One of the obstacles to upgrading is caused by systems built before today’s 32 or 64 bit platforms. Windows 7 and later minimum requirements, listed below in Figure 5, create the obstacle.



1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor
1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)
16 GB available hard disk space (32-bit) or 20 GB (64-bit)
DirectX 9 graphics device with WDDM 1.0 or higher driver.

Figure 5. Windows 7 Requirements from How to Upgrade (CCS, 2014).

Upgrades require vendor compatibility as well. Industrial organizations often depend on systems with code developed before Windows 7 (CCS, 2014). This means much of the supporting vendor

software remain dependent on the older OS. Vendors without compatible versions for the new OS will require other software upgrades in addition to the operating platform (CCS, 2014).

Infrastructure catastrophes. Aims to reduce catastrophe use lessons learned through practical exercises or incidental occurrence as teaching points. The lessons learned inevitably fail to demonstrate the technological shortcomings that are present within society. Historical examples ranged from maritime transport, aviation, deep-water drilling, and space exploration (Cavnar, 2010, pp. 49-53). Misguided Titanic engineers ignored their practice and followed executives seeking appearance and accessibility. Though design, structure, navigation, communication, and safety advanced afterward, it came at the cost of over 1500 people (Cavnar, 2010, p. 49). Another case is the Deepwater Horizon blowout in April 2010. Maintenance errors, coupled with miscalculations in the well's design and blowout prevention system's capability, allowed a manageable problem to evolve into an environmental disaster (Zatarain, 2015). Though these incidents did not stem from cyber related attacks, they represent the severity of the widespread impact resulting from infrastructure disasters. The practice of overlooking security in its relation to safety is a common occurrence that can result in equally disastrous events.

The explosion of the Siberian pipeline in 1982 is comparable to the scale of a nuclear detonation (The Archive, 2013). This is an example of a catastrophe relatable to an attack on a SCADA facility. Some viewpoints consider this event as the first known act of cyber warfare. During the era of the cold war, the Soviet Union had established an intelligence espionage operation. A Soviet defector exposed the espionage operation. The counter-intelligence that followed is said to have included fallible code for IC's which was incorporated by the Soviets in the Siberian pipeline project (The Archive, 2013). Although the explosion claimed no casualties, it caused ramifications for the Soviet economy (Loney, 2004).

In Arizona, the Roosevelt Dam incident in the 1990's, concerning a young man who compromised its ICS by gaining control over its SCADA servers, is another instance (NATO Science for Peace and Security Series, 2008). A disaster caused by a SCADA cyber event with the Roosevelt dam could inundate Phoenix, Arizona with 1.6 million acre-feet of water. The United States' fifth largest city would have only a few hours to evacuate 3.7 million people (Bommersbach, 2006).

As another example, reflect on an assault that overcomes the telecommunication system governing airline transportation. A 1997 incident linking a juvenile with the Worcester, Massachusetts Airport represents an event where interrupted phone service for safety and security resources demonstrates a significant potential for calamity (NATO Science for Peace and Security Series, 2008). An airport could face disaster when response capabilities and operational provisions are unavailable.

A staged event in November of 2013 known as GridEx II indicated the damages that result from a cyber-assault on electrical infrastructure (Wald, 2013). The resulting details serve as validation that ICSs are vulnerable, and that the nation's CIKR are at risk. Results from the drill indicated a loss of power for tens of millions, hundreds of damaged or destroyed transmission lines and transformers, and an ICN infected with malware still running processes (Wald, 2013).

Potential impact. Hypothetical constructs and practical scenarios are the only result of the deficiencies correlated with SCADA and ICS's. Moreover, although Government has worked to prepare for a cyber-incident, the information presented by simulated damages shows the Government's attempts to prepare for cyber incidents are unsuccessful. A singular attack could equate to economic and physical losses. This raises some questions. Multiple events happening

simultaneously as they unfolded on 9/11 overwhelmed emergency resources. The length of time required for recovery for 9/11 has exceeded a decade. The nation is not prepared for secondary conditions resulting from a multi-incident cyberattack similar to 9/11.

Defense Secretary Leon Panetta stated that a cyber-assault equivocal to 9/11 could be destructive and leave the nation incapacitated (Kerr, 2013). Security experts specify the time since 9/11 is a waste. Opponents argue desired improvements for funding is the reason behind such statements. The cybersecurity community is aware of the catch-up required (Clayton, 2014). The legislation and needed workforce mirrors the gap between security and SCADA assaults. Now referenced as the “lost decade,” the progress is minimal and a number of ICS’s are accessible on the Internet, unprotected from hackers, and deficient in security (Clayton, 2014).

Voluntary cooperation is necessary for mitigating incidents. Acquiring incentive by developing sound security practices within the private sector should be the focus (U.S. DHS, 2011). DHS recognizes specific categories of impact to quantify loss. Categories of impact for consequence are human, economic, public confidence, and government functionality (U.S. DHS, 2011). A well-positioned attack can affect all these categories. Accomplishing an attack by targeting the concentration of people on an urban public transport system is achievable by maximizing an attack with minimal resources (Al-Askandrani et al., 2013).

The perspective on the interconnection and reliance between different sectors of CIKR is underestimated. The interdependency of critical infrastructure becomes more complex daily and the functions of these utilities are a necessity for societal continuance (Huler, 2010, p. 216).

Figure 6 presents this interconnection.

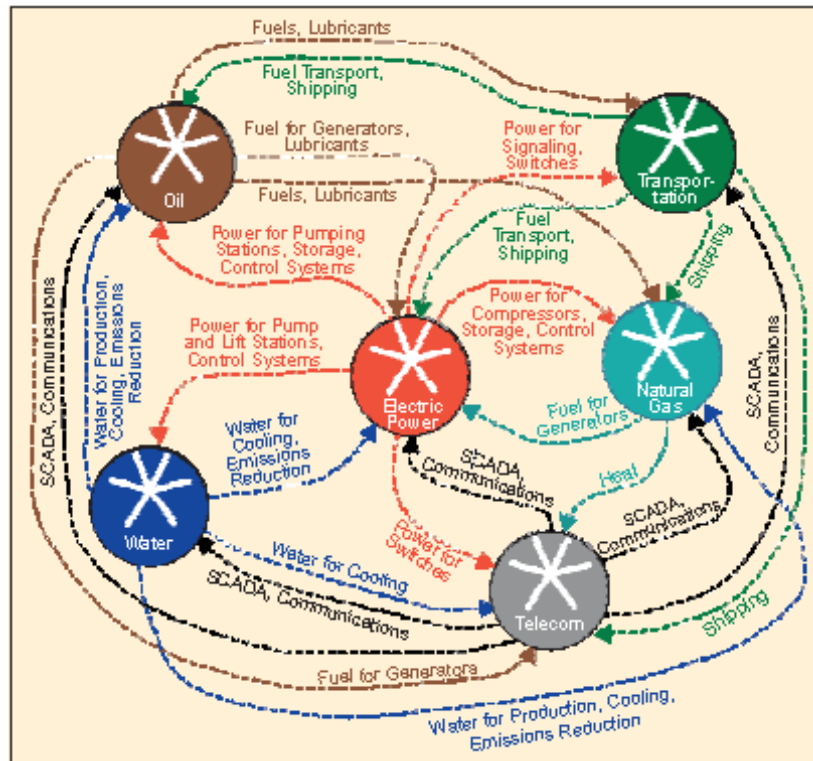


Figure 6. SCADA interdependencies by Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies (Renaldi et al., 2001).

“They are all complex collections of interacting components in which change often occurs as a result of learning processes; that is, they are complex adaptive systems” (Renaldi, Perenboom, & Kelly, 2001, p.13). Attacks on interdependent infrastructure can cause cascading effects. “What happens to one infrastructure can directly and indirectly affect other infrastructures, impact large geographic regions, and send ripples throughout the national and global economy” (Renaldi et al., 2001, p.11).

Mitigating IC Vulnerabilities

Service vs. security. The constructs of service before security led to the development of OPC-UA architecture. Business proficiency pushed improvement of the original design of Object Linking and Embedding (OLE). The development of OPC-UA came about for the provisional layer of common interoperability, information exchange, and process orchestration (Massaro, 2008). As a result, ICS’s acquired a service above security vantage deficiency. Industry

requested developers to integrate diverse information trees and unify Data Access (DA) with Alarm & Event (A&E) for a singular methodology because of the difficulty attributed to dual data sets between A&E and DA servers and intent to ease data reconciliation (Luth, 2004). This has moved ICS's to Internet accessibility, further complicating security and opening the door to event falsification and IC reprogramming techniques.

Service Oriented Architecture (SOA) made remote software applications available for use in ICS's (Paine, 2008). Remote capabilities allow external access to ICS's via the Internet. Original ICS designers intended to deliver meaningful layouts though many systems suffer from the common problem of poor design and diminished reliability. Some flaws are inherent, while others include by poorly executed field modifications when onsite staff may be less knowledgeable of critical aspects within these systems (Zatarain, 2005). OPC-UA technology requested integrated ICS's and delivered them to the Internet's platform of insecurity. Because the design of the Internet is for research and packet transfer, cyberspace has several technical failings and vulnerabilities. Keeping systems subject to its design secure is improbable (McCusker, 2006).

Acquiring improved security for CIKR organizations through the government's voluntary strategy has had little participation (Harwood, 2012). Since there is no mandate, these organizations choose to handle their own security. Without oversight, no determination can be ascertained as to vulnerabilities for such sites. Reasons related to non-participation are current government regulations and liability pertaining to associated risks (Harwood, 2012). The DHS has developed a CIKR requirement book to deliver comprehension about the requirements process for operational necessities (U.S. DHS, 2010). While the book may serve those who employ its resources, there is no guarantee of its use.

Corporate vs. industry. Evaluating corporate perspectives against those of industry provides an understanding of the difficulties of mitigating risks within ICS's. Relating corporate versus industrial decisions is possible through review of the Basic Control Loop. Shown in Figure 7, the Basic Control Loop presents the important aspect of control.

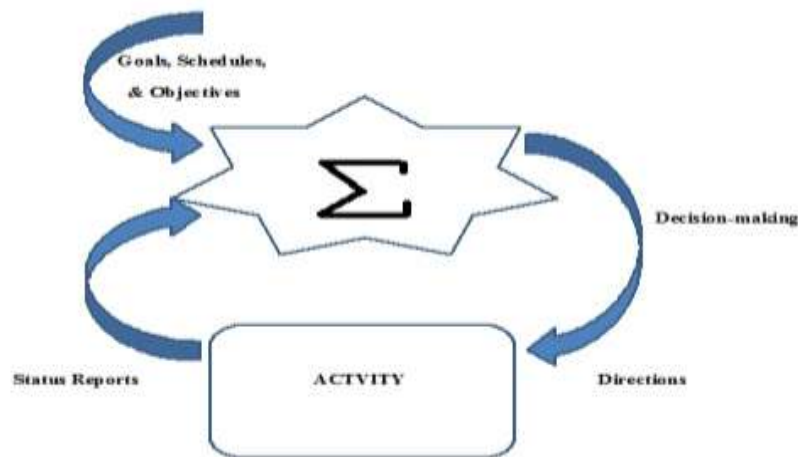


Figure 7. Basic control loop recreated from On the Structure of Operational Control Systems (Carroll, 1966).

Maintaining control occurs through the decision and information process whereby the absence of either reduces efficacy (Carroll, 1966). The operational cycle handled by the control loop indicates that influences for a task come from the corporate and industrial levels. In order to allow business management software to forecast maintenance trends and monitor performance corporate leaders have placed these networks at risk (Lynch, 2012). Corporate decision-making has overlooked the vulnerability of these networks when mingled with enterprise data. While economics is a factor for consideration, failure to weigh continuance of the physical attributes of maintenance and development does not complete the loop. Consideration of the full system is precedent (Carroll, 1966).

Ensuring networks are secure from the engineer's perspective has surpassed the simplicity of systems known three decades ago. Previously, an engineer had no need of IT concepts or knowledge of using human machine interfaces. Unrealistic expectations for prospect

engineers of CI span multiple fields and concentrations. Figure 8 displays a job listing by the City of Tacoma.

QUALIFICATIONS:

The ideal candidate will have a Bachelor's degree in Electrical Engineering, computer engineering, computer science, or closely related field and three years of progressively responsible experience in secure systems engineering, cyber security analysis, incident response, and SCADA experience

Figure 8. Job Qualification by SCADA Network & Cyber Security Engineer (City of Tacoma, 2014).

Human Resource departments are developing job descriptions that touch several professional fields where a singular application is probably not suitable. Table 1 displays the separation of requirements between ICS and IT technicians.

Table 1

Challenges for Control Systems

CRITICAL DIFFERENCES	CONTROL SYSTEM REQUIREMENTS	OFFICE IT SYSTEM REQUIREMENTS
Security skill/awareness	Usually poor	Usually high
System lifecycles	15-25 years	3-5 years
Patching	Slow/impossible	Frequently used
Computing resources for devices	Low	High
Administration	Localized	Centralized
Security impact	Potentially life-threatening	Potentially business-threatening
Timing	Critical	Not necessarily important

Note. By *Control System Cyber Vulnerabilities and Potential Mitigation of Risk for Utilities* (Juniper Networks, 2010).

Today, an engineer is responsible for safe and dependable layouts inclusive of risk analysis as well as communication and control principles (Lusignea, 2013). In terms of the corporate vantage, complications causing service outages due to manual changes result in security being ignored (Lieberman, 2012). Declined invitations and involvement in security assessments

provided by the DHS indicate cybersecurity ignorance within CIKR organizations (Harwood, 2012). Investments to protect ICS's against vulnerabilities have been minimal (Moore, 2010).

Profits drive corporate business views. Placement of profits above service continuity is a ~~perception policy~~ that is generally ~~altered alters~~ only because of adverse publicity (Alexander, 2011). Much of all code produced does not receive the reliability consideration that it should. Though the issue may be new to engineers working with ICS's, the problem has been relevant since the writing of the first software code (Alexander, 2011). The issue is a known deficiency for corporate leaders as "Patch Tuesday" is now a common term. Engineers and operators depend on corporate executives to provide them with reliable tools. Those ICS executives that fail to demand better code from vendors, compound system vulnerability. The pace and complexity of threats require senior executives to confront these problems while retaining innovation and growth (Kaplan, Sharma, & Weinberg, 2011).

Typical security technology. Unlike a typical IT network, an ICS network does not need exceptional throughput. However, an ICS is far more time-critical, with each specific installation detailing tolerable levels of delay (Fergus, 2009). Their need to remain self-sustaining is significant. Unforeseen outages are unendurable and the systems' continuous nature demands availability (Fergus, 2009). The ICS system platform is fragile in terms of standard IT Security. Integrating the ICS with defense capabilities such as antivirus or intrusion protection in real time is not possible due to its vulnerability to network manipulation, disruption in timing, and specific need of expertise (Fergus, 2009). Table 2 indicates the differences between standard IT networks and the typical ICS network. The basis of security relies upon the premise of Transmission Control Protocol and Internet Protocol (TCP/IP). The growing reliance on IT technologies has made it easier to interface with ICS's and reduced their previous isolation from network attacks

(Byrnes, Franz, Carter, & Peterson, 2007). This improved technology attaches greater risk and the benefits require deeper concern. Highlighted below is the complexity of the problem

It is our belief that the most serious issue for OPC is that configuring OPC applications securely have proven to be a major challenge for most engineers and technicians. Even though OPC is an open protocol with the specifications freely available, users must wade through a large amount of very detailed information to answer even basic security questions. There is little direct guidance on securing OPC, and our research indicates that much of what is available may actually be ineffective or misguided. Overall, there is little doubt that some clear advice would be very useful for the control engineer on how best to secure currently deployed, COM/DCOM-based OPC systems. (Byrnes et. al., 2007, p.6)

Until recently, the standard IT enterprise security posture was the only application to devise defensive applications for an ICS. Use of firewalls, encryption, authentication measures, and other common metrics do not perform as efficiently for industrial platforms. Firewalls, the primary restrictive component for locking down networks, do not provide adequate utility to defend against industrial threats. Tofino Security has constructed a security appliance for IC's which restricts all traffic except that specifically stated by the appliance (Tofino, 2013). With this device, the IC has its own firewall. Tofino's design also allows engineers to devise and develop security zones within its flexible hardware/software product when deployed across an ICS. The application seems to afford promise, yet other opinions exist. There is no single solution to apply complete defense for ICS networks (Jacobs, 2013). Jacobs states that understanding the total scope is important. Product purchase will not solve cybersecurity issues; risk assessment is the starting point (Jacobs, 2013).

ICS configuration weaknesses. The presets for ICS's are another distressing factor. A common weakness exists for many modules. Their Ethernet cards have hard-coded default passwords that are easily found in published support manuals (Paganini, 2012). Patches cannot fix these hard-coded faults; retirement of the hardware is required to mitigate the problem (Paganini, 2012). With the coming advances, vulnerabilities will expand. The electric grid configurations will require more communication control capabilities introducing added access points (Craig Jr. & McKenna Jr., 2012). The exposure of these networks will increase. Due to the deployment of smart meters, intelligent appliances, and other sensors the number of managed devices within residences will expand to between ten and a hundred (Craig Jr. & McKenna Jr., 2012). Adjacent to vulnerability caused by exposure is interconnectivity. Bridged heterogeneous networks will create risks extending from the linking of those networks (Craig Jr. & McKenna Jr., 2012). Wireless integration continues to move forward with many circuit boards having the antenna printed on the board (Zwan, 2010). Complex systems will become more complicated. Increased complexity will further stress systems with the implementation of more points of failure (Craig Jr. & McKenna Jr., 2012). Standard IT risks will multiply. The added necessity of common computing technologies such as multipurpose operating systems and routable networking will increase problems prevalent in the office environment (Craig Jr. & McKenna Jr., 2012). Manual operations will decrease. Those decreases will lead to more automation which amounts to compounded risks (Craig Jr. & McKenna Jr., 2012).

The North American Electric Reliability Council (NERC) has noted the top ten vulnerabilities for ICS's. These weaknesses are scaled as foundational, intermediate, and advanced and range from policy and procedure issues, problems with wireless networking, insufficient detection and reporting metrics, and more (NERC, 2006). The vast amount of

information available on the web provides access to complete libraries of vulnerabilities such as those at SCADAhacker.com (SCADAhacker, 2014).

ICS network weaknesses. The introduction of ICS networks to the modern perspective of business operation has presented many of the aforementioned security concerns. Their environments have been modified to consider commerce and trade first and leaving likely security effects with little regard (U.S. DHS, 2011). The lack of attention dedicated to security leads to more problems. The lack of focus for defensive measures introduces gaps in a system that without remediation may become back door access points (U.S. DHS, 2011). Visits conducted to ICS facilities due to response and assessments have revealed these vulnerabilities. Noted among these architectures is missing defense-in-depth deployment, zoning, little if any port security, and weak access control. The architectures are in parallel connection with corporate networks absent firewalls or demarcation zones (DMZ) to assist in protection from the Internet (U.S. DHS, 2011). Networks that exhibit the most exceptional risk should have well-define security perimeters. Segmentation of these networks would limit immediate access during attacks. Configuration for firewalls should restrict data to appropriate network locales. Application of DMZ's to large architectures can help to isolate roles and privileges. Removal of Available bypass access points within the ICS that allow firewall avoidance must occur. To further compound the weaknesses with ICS networks, audit and accountability practices are frail. Related to this matter are incomprehensible network architectures, minimal enforcement of remote authentication, media egress control, and poor intrusion detection monitoring (U.S. DHS, 2011).

Resilient Systems

AI obstacle. Two issues with advancing AI usage are the lack of extensive knowledge base capabilities, and the ability to learn. The element of complexity appears to be that an AI system must retain a vast spectrum of knowledge and traits that allow it to write programs for specific conditions it cannot answer. AI experts note that problems with artificial intelligence and involved programming technology are so complex that algorithms and standard programming methods are insufficient to solve them (Sammet, 1971). Although this argument bares truth, it does not detail the advances in AI.

Other opponents or arguments against AI have noted problems pertaining to memory capacity and order. Advance knowledge of information storage requirements and memory organization infers that programs need flexibility (Simon & Newell, 1964). These perceptions introduce a state of stagnation with AI. Artificial Intelligence (AI) advancement made ground early on but has had less concentration and research because of the impacts of these observations and the belief in the condition of system restriction.

Expert systems are unreliable when confronting problems outside their respective areas and, therefore, may provide incorrect answers in those situations (Nilsson, p.407). Because the sciences of molecular biology and neuroscience still lack comprehension of the physical mechanisms responsible for human cognitive function, AI may remain restricted until more revelation of those fields of knowledge (Moravec, 2009). Experts in the field determine a successful AI system will be able to pass the Turing test while others argue behavior testing proves no cognitive skill (Vincent, 2014). Early on, Information Processing Languages (IPL) and algebraic languages received criticism for those conditions related to the very same ideals (Simon & Newell, 1964).

The ability to construct ICS's capable of handling the adversity presented by their connection to the Internet depends upon a constant dedication to AI programs. Future perception for AI should focus on the singular purpose of a required task, similar to methods of today's software designs. Adoption of heuristic concepts in programs can offer future acuity for AI advancement. Chess programs match human ability, exceed checkmating amalgamations, and show identification of human problem solving abilities for provision of "means-end analysis" required of theorization and formation in computational processes (Simon & Newell, 1964). Research and investigation of heuristic concepts is what allowed AI to reach its current status. Effort must be made to teach programs to learn from incident and write code for itself. AI must bridge this gap to achieve benefit for IC's.

Precepts that AI achieved its roots due to upheaval against limitations in present fields have caused regression in its advance (Russell & Norvig, 2010). Such regression is isolating information security from defensive constructs required by ICS's. As noted by David McAllester, automated reasoning is inaccessible from proper procedures and fixed analysis (Russell & Norvig, 2010). Overcoming the regressions and limitations found within AI is conceivable with resilient control applications. Such an approach does not leave ICS defense to reactive response, rather provisional of proactive measures (Rieger, Gertman, & McQueen, 2009).

Resilient control systems. Resolving the current enigma within Critical Infrastructure (CI) depends on resilient designs. Designs of current systems depend on operator reprogramming and or repair after the fact. By designing systems that consider all threats and measures, the problems confronted in CI can be alleviated (Rieger et al., 2009).

The dated definition of resilience fails to consider the current state of security for CI. The ideology of organizational and information technology in association with resilient systems are problematic. A terminology that suggests systems can tolerate fluctuations to their structure and parameters fails to account for malicious deeds (Rieger et al., 2009). One alternative is the idea of Known Secure Sensor Measurement (KSSM). “The main hypothesis of the KSSM concept is the idea that a small subset of sensor measurements, which are known to be secure (i.e. cannot be falsified in the physical layer), has the potential to significantly improve the observation of adversarial process manipulation due to cyber-attack” (Linda, Manic, & McQueen 2012, p.4).

Resilient systems should be able to determine uncertainties, sense inaccuracies under all conditions, take preventive action, recover from failures, and mitigate incident beyond design constraints (Yang & Syndor, n.d.). Valid resilience considers representations of proper operation within process applications when facing varying conditions inclusive of malicious actors and includes state awareness within the resilient design (Rieger et al., 2009).

System resilience in current CI architectures is dependent on human reaction and analogy. While human capability delivers sound heuristics and analogy, certain situations can arise connected to fatigue, stress, or other human deficiencies that affect decision-making quality (Rieger et al., 2009). Further complexities are relevant in the use of digital technology. Breadth of information for operator response and the automated versus human manipulated inputs or combinations thereof present complex interactions that leads to a lack of clarity in dependencies and rules (Rieger et al., 2009). True resilience requires a system to function with a comprehension of these variables. A resilient control system will be error tolerant and complement the system with perception, fusion, and decision-making (Rieger et al., 2009).

Prediction of failure has been successful where systems employ fault detection, diagnostics, and prognostics (Yang & Syndor, n.d.).

Cyber awareness. Awareness in the cyber domain intended governing to happen through risk assessment. Only forensic evaluation after the fact truly indicates the actual cause of an abnormal event (Rieger et al., 2009). Predictability in determining critical digital assets is difficult to impossible in regard of hidden dependencies (Langner & Peterson, 2013). The intellectual aptitudes of malicious actors improve through the usage of stochastic methods whereby variability of motive and objective exist (Rieger et al., 2009). Put simply, risk management allows no technical review of potential risk and is really a business tool (Langner & Pederson, 2013). A huge misnomer resides in the condition that risk mitigation will allow defensive metric implementation in ample time. Cross-reference this with CI and the idea is flawed.

Rapid reconfiguration in these environments is not a possibility; due to their design, the probability of mitigation is near impossible (Langner & Pederson, 2013). Though routine and common pattern analysis may provide anomaly comparisons, its limitations in predicting an adversary's behavior is minimally effective (Rieger et al., 2009). The three principles provided in Table 2 should be the basis for policy and the way forward.

Table 2

Basis for Policy

Basis for Policy
Principle 1: Primacy of Politics- CI protection is a political issue
Principle 2: Practicality- Fix design vulnerabilities/ avoid hypothesis
Principle 3: Pervasiveness- Cybersecurity need not be restricted to CI

Note: by Bound to Fail: Why Cyber Security Cannot Be "Managed" Away (Langner & Peterson, 2013, pp. 9-12)

Viewing CI from as a political issue is precedent. Fixing design vulnerabilities should be paramount and should not include hypothetical solutions or assessments. Though CI is vital the security of the cyber domain should be viewed unilaterally.

A resilient control system must have the capability to counteract malicious attack because such systems are digitally based and thereby more vulnerable (Rieger et al., 2009). Business logic values risk-taking over resource spending and since critical asset owners often find a rationale for doing nothing when surveying systems with risk management, they are quite happy with the expenditure required- nothing (Langner & Peterson, 2013). Such practice negates improvement for CI and the ability to build resilient systems.

Data fusion. Gathering a scope on data integration presents the obstacles that restrict AI in CI environments. The consumption of data determines information generation and appropriate judgment of that information (Rieger et al., 2009). Implementation of data fusion through a centralized application can accomplish reasoning of heterogeneous information and allow adequate countermeasures to be triggered (Flammini, Gaglione, Mazzocca, Moscato, & Pragliola, 2008).

Insight on the definition of data fusion aids in the comprehension of its inclusion. Valid effects demonstrated through experimental process on simulated SCADA systems prove autonomous sensory agents report successfully to a central processor to fuse evidence from physical and virtual dimensions to provide a unified view of the system. (Genge, Siarerlis, & Karopoulos, 2013). Synthesizing raw data from multiple sources allows generation of better information (BusinessDictionary.com, 2014). Data fusion can help with areas of AI recently found restrictive.

The attributes connected to data fusion principles provide the related potential. AIIC will understand how to sift through data and reduce nonessential information. The principle of identification gives AIIC validation ability. The knowledge base will continue to progress over time through usage of the improved characterization and knowledge principle. Data fusion provides attributes whereby AI can advance CI security as seen in Table 3.

Table 3

Principles of Critical Infrastructure Security

Principles for Critical Infrastructure Security
Reduction - The reduction of data to provide only that information necessary for the human or automation scheme to provide the appropriate response, i.e., to prevent a common issue of information overload.
Identification - Validation and invalidation of causes for events, e.g., a process upset is due to a failed valve and not a cyberattack.
Improved characterization and knowledge - Development of new information that helps to better characterize the process application, e.g., mining of process temperatures along with process flows provides a better interpretation of stability.

Note: by Resilient Control Systems: Next Generation Design Research. (Rieger et al., 2009, p. 4)

The usage of data fusion has the ability to improve alert and proactive measures for CI systems.

Use in ICS's can achieve robust structures whereby they combine fusion and analysis; security and privacy; and collaboration and information sharing (Informatica, 2013). Such technology is beginning to provide large quantities of data. Interconnected industry delivers vast information pools from perimeter and network security systems (Informatica, 2013). Achieving robust systems starts with enabling a network to sense attacks and indicates such with warning indices through supported data fusion, accomplished through the management of intrusions, misuse, anomaly detection, diagnostics, and pattern analysis (Chairman of the Joint Chief of Staff, 2012).

Simplifying intelligible design. Humanity is absent assurance of creation, whereby speculation between theology and evolution govern the debate of intelligible design (Grinnell, 2009). Without focusing on the former, the intent is to encourage simple intelligible designs.

Success with complex intelligible AI designs becomes exhausting and it taxes human innovation due to the difficulties of mimicking the neuro physics of the human brain (Salamon, Rayhawk, & Kramar, 2010). Such complication indicates the direction where AI is more productive.

It is still speculative as to whether computers enable learning more effectively rather than traditional programming techniques (Keller, 2013). There is belief, however, that an artificial general intelligence (AGI) system, given correct rudimentary basic abilities, could learn perceptual patterns through different sensory perception among diverse environmental contexts (Voss, 2002). Debate revisits the premises that AI cannot advance without a connected neuro network, sensory perception ability, and an encoded knowledge base (Hayes, 2012). Adaptive and flexible attributes within AI entities have achieved conceptual goals, though efficiency across the broad spectrum of human knowledge and self-awareness is elusive (Voss, 2002). Since ICS security is a specific goal, AI should prove beneficial.

A lack of further development may find explanation in the intent to achieve simulated consciousness and its detachment from the cognitive continuum (Gerlenter, 2007). Advancement for AI may reach accomplishment through singular purpose concepts such as the success of Vicarious' recursive cortical network in passing the Captcha test (Johnson, 2013). Vicarious' work to skip past human brain emulation is where it associates this achievement. Broad-spectrum knowledge depiction requires ontology to link the variable domains of knowledge (Russell & Norvig, 2010). Ideas adapted around flexible modular frameworks tailored to specific networks could achieve target goals and help to grow the knowledge base needs of AI advancement (Sowa, 2002).

Involving fuzzy logic, an AI subset designed to capture expert knowledge and perform decision-making, is suitable for nonlinear systems such as ICS's (Dingle, 2011). While science's

current attempts are not effective in creating conscious intelligence this should not restrict those innovations and continual advancements in unconscious AI programs (Gerlenter, 2007). For the purposes of further clarity and comprehension, the concept of unconscious AI relates to a system that is not self-aware.

Discussion of Findings

The purpose of this research was to propose increased role for Artificial Intelligence (AI) for adaptive measures in cybersecurity for Industrial Controllers (IC) to provide Resilient Control Systems (RCS) and improve cybersecurity for such devices. What factors indicate a need for advanced security in industrial controllers in current systems? How can AI mitigate vulnerabilities and threat levels to Industrial Control Systems (ICS) and critical infrastructure? How will AI improve IC to introduce RCS?

The concept of improving security for IC with artificial intelligence within RCS has rationale. The advancement of security for IC's in current topologies is necessary. Improving ICS's that regulate CIKR can potentially mitigate vulnerabilities and reduce threat levels through the introduction of Artificially Intelligent Industrial Controllers (AIIC). The improved state awareness of an AIIC should improve ICS's and produce RCS. Revisiting the particulars of the relevant research questions here reveals the upshots of AIIC.

Governmental Incompetence

As General Keith Alexander alluded to, all networks including CIKR require protection. Evident among the problems to accomplish protection is the inability of governing entities to manage CIKR (Roulo, 2014). The U.S. Government Accountability Office (GAO) introduced the detached perspective of the Department of Defense; the report dictated a failure to complete departmental assessment, capability gaps, or implementations to handle such gaps (US

Government Accountability Office, 2011). The GAO detailed a failure to commit to the problem and the position these efforts have caused for CIKR. Other studies indicated bleak comprehension of cybersecurity by federal investigators. Sixty-three percent of federal agents examined in the study fall into an incompetent classification, the other thirty-seven percent lacked adequate networking and counterintelligence abilities (Mick, 2011). Dedicated effort must extend to improve CIKR legislation and knowledgeable personnel.

The major handler of CIKR is the private sector. Security advancement for such information systems will remain difficult without oversight. The federal government admits to the vulnerability caused by self-reliance. Many of the tough questions to ensure NIPP and the partnership strategy devised by the government become productive, seen in Table 4, need answering.

Table 4

Tough Questions for Cybersecurity

Questions for Cybersecurity
How responsibility and accountability are to be apportioned between government and industry?
What obligations each side will have to share sensitive or proprietary information with each other?
Who will monitor the performance of each party, and what criteria for evaluation will they use?
Who will provide the resources required for addressing the security externalities, including organizational reliability, that each side believes the others should cover?
Who will be held liable after the next disaster, and to what extent?
How will economic losses be compensated and who will pay for them?
Up to what extent will taxpayers and consumers (and investors) be willing, over an indefinite period into the future, to pay for increasing public security?

Note: by Seeds of Disaster, Roots of Response How Private Action Can Reduce Public Vulnerability. (Auerswald et al., 2006, pp. 157-163)

These questions outline were the NIPP strategy lacks the ability to garner private sector rapport and support. Furthermore, the U.S. government confirmed the susceptible condition faced by ICS networks. The entities managing these systems want solutions while avoiding the required expense. Private sector risk management strategies retain an unproven technique

whereby the necessity for intervention becomes relevant. Predictions based on negative consequences related to cyberattacks show business decision makers the difference between costs of consequence versus mitigation – it creates false encouragement in risk-taking over resource spending (Langner & Pederson, 2013). The truth of the matter is that risk management is an unproven technique. Government and ICS organizations do not have sufficient personnel and look to invalidated practices for security measures.

Growing Target Topology

The NSA has described losses caused by cyberattacks as $f = (a_a)(f_e)$ (a function of achievable action and expected frequency) later referenced as the Davis Cyberattack Loss Equation (Davis, 2014).

$$f = (a_a)(f_e)$$

Figure 9. Davis Cyberattack Loss Equation devised from A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS) (NSA, 2010). (Davis, 2014).

Lowering achievable action and or expected frequency would eliminate losses. The complexity of reduction becomes relevant by the ability to restrict achievable action and expected frequency. Only one condition of the equation is necessary to accomplish the attack. The potential of an attack, however, has more possibility with a combination of the entire equation. Successfully minimizing the targeting of ICS's may be conceivable by exploring those techniques that eradicate the facets of those functions necessary for cyberattacks. Focusing on these conditions initiates ideologies necessary to devise RCS's.

Conditions are prevalent that represent the ability to hack CI. The potential for attack exist from its interior, exterior, from state-sponsored actors, accidentally, or simply from the criminal element. Charting the data recorded by the U.S. Computer Emergency Readiness Team from 2013 using the Davis Cyberattack Loss Equation presents the scope of the problem. It is

also important to remember that the frequency recorded only charts half the year. Figure 10 details the critical condition of CIKR and the affect that an increase in the Davis Cyberattack Loss Equation could include. Consider the interdependent disposition of CIKR and the condition is likely to reach a terminal state.

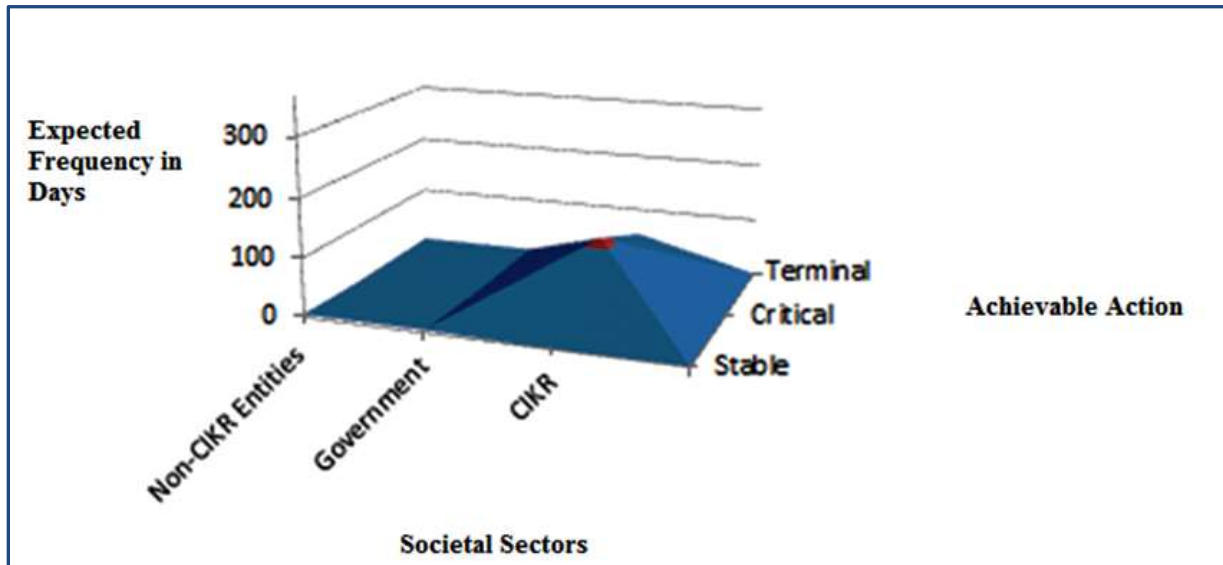


Figure 10. Effects of Cyberattack Loss created from ICS-CERT Monitor and the Davis Cyberattack Loss Equation (Davis, 2014).

Antiquated systems magnify the problem because these systems do not respond well to standard IT protocol and may face damage. Revamping ICS's with standard IT defenses can cause damage or destruction to commodities and/or irreparable damage to those systems. Modbus devices are reachable and vulnerabilities are increasing.

Conditioned for Exploit

SCADA industries are an interwoven network of interdependent entities; this makes them a target rich environment. Stable societies rely on SCADA. Cyberattacks occur on these networks. Appendix A, presented previously, illustrated that such exploits occur at least 2.4 times a year. Expansive field stations that broaden and divide defensive capabilities provide access points for nefarious individuals.

Software vulnerabilities known as “buffer overflows” have shown an ability to open backdoors to ICS’s. This type of access is achievable through ingenuity and traffic monitoring. Even with the application of firewalls such attacks are successful (Udassin, 2008). When the buffer experiences an overload of data, adjacent memory allocation takes place. The displacement allows injected code to run with the privileges of a vulnerable program and obtain control over kernel functions (Cowan et. al., 2000, p.1). Open source sniffing software such as Wireshark, tcpdump, and netcat divulge details about targeted systems easing such practices. The advance of information technology means most systems are antiquated and the code used within these platforms introduces exploitable venues. The red line in figure 11 displays the progression and areas a hacker would use to infiltrate and attack an ICN. Loss of power would be the resulting failure if the target were an electric turbine generator. In conjunction with the population, those connected CI components depending on that power would also suffer issues.

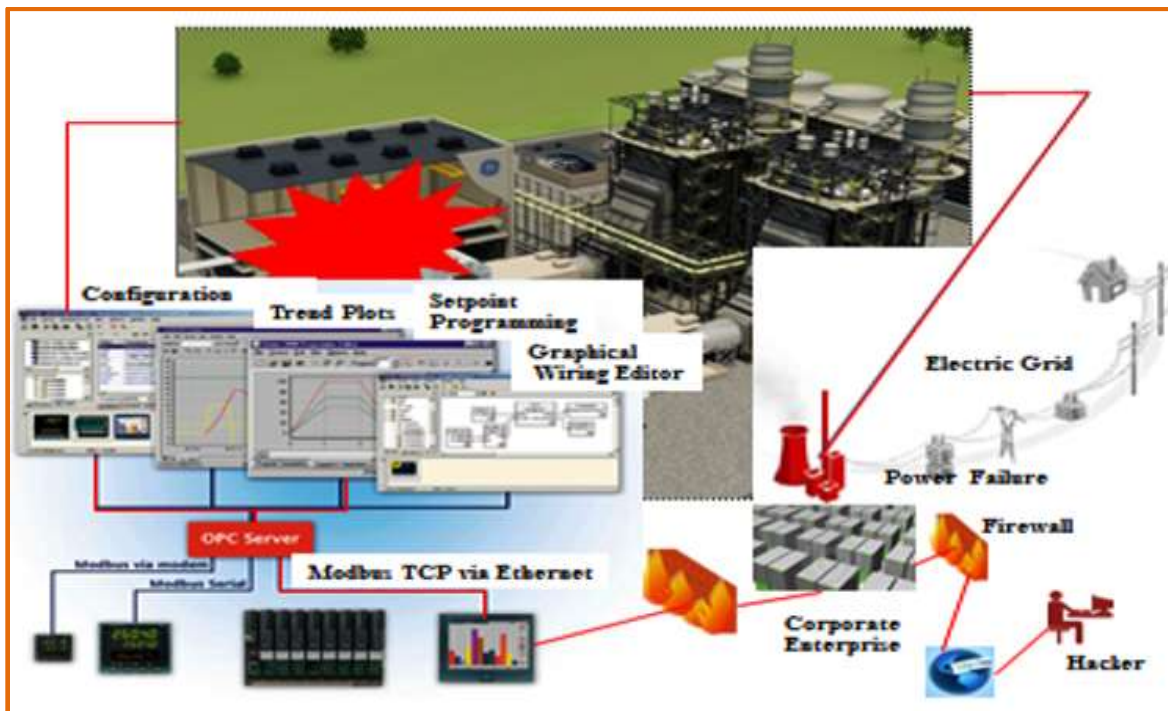


Figure 11. Electric Turbine Cyberattack

Failure to Upgrade

Roughly, 4.9 million systems still use the Windows XP operating system. The eighty percent of Britain's National Health Service still using Windows XP reinforces this declaration (BCS, 2013). Vulnerabilities to Windows XP systems that still manage CIKR become relevant. China's resistance to migration and the improved potential for security threats illustrates the significance of vulnerability in systems that continue to use older platforms (Ramzy, 2014). This is where oversight can assist in security practices. Most notably, the banking systems of modern society should note the dangers in allowing outdated operating platforms to control automated banking provisions. Bloomberg Business Week's information documenting 90% of ATM machines still using Windows XP highlights this problem (F-Secure, 2014, p. 16). Alternatively, other CIKR organizations dependent on software upgrades for non-compatible vendor software may find themselves in a precarious position. The largest percentages of systems using the outdated platforms are associated with point of sale (POS)/ retail, financial services, and infrastructure (Shook, 2014). Vendors are failing to meet the needs of an evolving technology and society. Vendors must begin a dedicated effort to modernize CIKR systems.

Minimal Risk Perspective

Cyberattacks and cyberespionage date back potentially as far as the 1980's. Since that date, several recorded incidents are SCADA specific scenarios. Incidents such as the 1982 Siberian pipeline explosion, the 1991 Roosevelt Dam network breach, the 1997 Worcester airport telecommunication disruption, and practical exercises such as Grid Ex II in 2013 show the risk perspective for SCADA incidents is minimal. The element of cyberwar and its potential shows relevance on global stages. Practical exercises and hypothesized SCADA catastrophes indicate the losses attributed to these issues brought to reality. Emergency resources cannot

handle problems when SCADA interdependencies overwhelm them in such situations. The scope and complexity of a SCADA catastrophe can be geographically exponential. Attempting to mitigate risk by assuming that worst-case scenarios are highly improbable is naïve. The vantage fails to calculate the cost or ability of disaster recovery given an incident becomes reality.

Depending on voluntary cooperation and participation to rectify CIKR's security gap is a dangerous venture. Information recorded by the Congressional Research Service details that less than three percent of the U.S. electrical grid consists of high voltage transformers, yet they carry approximately two-thirds of the nation's power (Parfomak, 2014). A coordinated assault on as little as nine similar substations could perforate the dependent structure of CIKR (Smith, 2014). It is important to note that this only assumes a scenario directed at one sector of CIKR. Although many indices provide details of vulnerability, business and government think tanks continue to hinge on mitigation and risk management techniques rather than prevention stratagem.

Prevention Not the Focus

The private sector has broadcasted its business plan. OLE increased the pace of business with minimal attention for mitigation potential or cost. Security only seems necessary when situations fall outside the requisites of risk management. Vulnerabilities multiplied for CIKR systems with the onset of Internet connectivity. SOA made remote capabilities an open door for hacking exploits. Declining expertise and outdated ICS designs magnify security problems. If prevention is possible, participation must garner diligent effort. The perception of ICS environments is that they have vulnerabilities within working components that may never be repairable whereby a resulting incident is understandably injury, life loss, or financial repercussions (U.S. DHS, 2009). DHS associates current regulations and liability with the lack of

participation in CIKR. If little participation exists after a decade of attempting to acquire contribution other measures should gain consideration.

Industrial safety inadvertently receives inadequate attention because most corporate leaders are not aware of the risks associated with cyber security. Any corporation's management plan will have better service when executives understand that much vulnerability is inherent to networked industrial control systems. Only then can they allocate adequate funding and processes that fully protect their assets to ensure ongoing productivity and profits in both the short and long term. It is improper to mitigate ICS vulnerabilities with individuals when a workable solution requires a [multi-discipline](#) team effort. One person cannot efficiently perform system engineering integrity, cybersecurity, networking architecture, procurement, planning, and design and successfully support the critical function of a SCADA system (City of Tacoma, 2014). IC engineer comprehension of current information security technology is assumptive and vice versa.

ICS communication technology is obsolete in comparison to enterprise communication technology. Absent efforts to improve vulnerabilities that face ICS engineers, future improvements are unlikely. Ensuring code reliability holds no importance, and ICS engineers cannot properly manage CIKR due to lack of tools. Moreover, the Emergency Services Sector (ESS) should direct attention to the fact that it is dependent upon CIKR as well. Recovery from disaster falls to the responsibility of ESS (InfraGard, 2014).

ICS Security Deficiency

Attempting to secure ICS's requires out of the box thinking. These networks do not allow standard IT security measures. Further, IT technology has outgrown the code used to program ICS's. The necessity of uptime and self-sustainment makes the provision of security

both critical and complex. Guidance to secure ICS platforms is negligible, and engineers have poor knowledge bases to depend upon. Firewalls, which are the primary component used to divide enterprise networks and their adjacent ICS's, are inadequate. Other deterrent physical applications such as Intrusion Detection/Prevention systems cannot provide a dynamic process to achieve cyclic analysis. Independent device deployment does not receive high rapport. Risk Management retains approval for risk mitigation.

Allowing cybersecurity to depend solely on static applications adds complexity to the problem. While additional deployment of AIIC may help, there should be a combination infused with dynamic cyclic processes such as ACDC. The compliment of human analysis across a spectrum of dedicated cybersecurity partitions delivers a strategic concept of active defense. The strategy also improves defense-in-depth. Absence of active defense metrics may make the concept of AIIC no better than other static applications because the technique intends to use AI in an unconscious concept. Combining active defense with AIIC could introduce expert knowledge databases where situation awareness and state awareness are parallel techniques working in harmony for ICS.

Configuration problems upend risk management techniques. Hard-coded default passwords found in published manuals allow access for anyone breaching the ICS network. Patches are not an option. Equipment retirement and replacement is necessary without a different approach. The constant advance of technology requires more communication meaning added access points. Management is not dealing with security margins caused by common off-the-shelf technology (COTS) integration into ICS networks (Zwan, 2010). Additional access leads to increased network exposure. Complexity for these systems will only increase meaning the ability to apply security will decrease. Amplified automation further compounds these risks.

The largest weakness for ICS networks hinges on commerce and trade placed above security. The DHS records many ICS network architectures as lacking defense-in-depth provisions. Though firewalls remain the best layer of security, deficient networks have no arrangement of well-defined security perimeters or segmentation as suggested by the DHS. Systems designed with remote access ability and simple password attributes allow compromise of authentication through brute forcing techniques (CERT Monitor, 2014, p. 1). Auditing and accountability do not find top consideration in networks where societal dependence is pivotal.

Need for Advanced Security in IC

This information details the necessity for advanced security in ICS within their current systems. Governing agencies can annotate the risks and deficiency of knowledge within their personnel. NIPP is dependent upon the ability to build rapport with the private sector who owns most of CIKR. Furthermore, unproven tactics protect these networks. The attack surface continues to increase, ICS structures retain prime availability for exploit, upgrades and or migrations are slow to nonexistent, the perspective of risk is inappropriate, and prevention is not a vital focus.

Evaluating AI

Artificial Intelligence development has been marginal recently. Learning abilities and restrictions associated with extensive knowledge bases reduce progress. AI requires knowledge base provisions that lack the breadth to allow a system to learn adequately or produce code. In situations where no answer reveals itself in an AI knowledge base, questions remain unanswered. AI has not acquired the abilities of expertise gained through experience or education and common sense or general knowledge attained through day-to-day existence in the external world that it could apply with little effort similar to human cognitive function (Nilsson, 2010, p. 407).

However, a system did recently pass Turing's original AI test showing grounds for advancement (Vincent, 2014). Improving AI requires better programming techniques and algorithms for the level of complexity involved. A computer-based neuro system capable of human-like functions or cognitive function remains below any standard of sophistication that could accomplish the associated purpose (Moravec, 2009). Another area necessary for improvement involves innovative data storage and memory organization. Lack of progress advancing the development of AI will continue without consideration of these factors.

Acuity for proposed AIIC is possible through consideration of singular purpose techniques. This level of awareness refers to AGI, the ability to achieve goals essential to domain specific knowledge (Voss, 2002). Procedure and analysis must not restrict automated reasoning potential. Achieving resilient control applications may break ground for AI in other areas. Developing AIIC's holds the potential to eradicate reactive response for the more desirable ability of proactive reaction.

The Reality of Resiliency

The perception that a system becomes resilient through enterprise and information technology organization is unproven. These systems continually face malicious action. Introduction of state awareness and proper operation/system understanding development is the only way to achieve proper resilience. Devising ICS's with a set of diverse performance criteria for maximum adaptive ability in response to cyber threats is the state awareness ideology where resiliency becomes beneficial to CI (Linda et al., 2012). Dependency on human reaction and analogy leaves fatigue, stress, and other human elements as potential points of failure in current resiliency constructs. Large information pools combined with the complex interactions of automated versus human inputs and combinations of both diminishes clarity for dependencies

and rules. Systems designed with perception, fusion, and decision-making abilities will provide resiliency.

Current resiliency and cyber awareness depends on the mainstream ideology of risk assessment. Finding the true origin of abnormal events comes through forensic evaluation. The missing element of technical analysis concerning potential risk reveals the truth of risk management. Adversary behavior prediction is improbable through pattern analysis. Valuing risk-taking over resource expense underestimates disaster recovery potential. Directing development and focus of ICS's in line with the concept of KSSM is a more realistic concept where systems may learn to monitor, analyze, and diagnose mitigation for cyberattacks. True resiliency for ICS's is unlikely under current risk mitigation perspectives.

Applying Data Fusion to CI

One of the detriments to AI is depth of scope within the knowledge base. Data Fusion technology holds inspiration that this obstacle can be breached. Applying data fusion within a centralized application provides heterogeneous comprehension and defensive discernment application. A combination of data fusion with analysis, security and privacy, and information sharing introduces abilities needed to make ICS's robust networks capable of sound defense. Physical application of predictive model techniques for anomaly detection can be beneficial during periodic analytical reviews of ICS's (Genge et. al., 2013). Use of data fusion networks could allow sensory notification and early warning. Large pools of data are already available from interconnected industry. The attributes of data fusion employ data reduction, event validation, and proper application characterization.

Merging CI and Simplified Intelligible Design

AI has focused repetitively on achieving intelligible design. The lack of understanding related to the neuro-physics of human cognitive ability impedes this achievement. This presents the area of productivity that should be the focus. The successes of AI on specific goals are not so elusive. Applying the power of successful AI tools from the last four decades can offer competitive hybrid ICS's and are applicable to assembly lines, robot, and low-capability microcontroller configurations (Sanders, 2013). Honing the scope of AI development for the singular purpose of ICS security may serve benefit and security for these networks. AI is clearly useful in specialized domain specific knowledge applications (Lewis, 1997, p. 35). Designing AIIC's with the innovation of modular structures for their specific networks holds promise to reach the goal of artificially intelligent ICS's.

Improvement in AI systems is occurring, although slow in its integration into industry, new developments create unified interactions for human and digital sensor systems (Sanders, 2013). An unconscious AI system that provides the provision of security sought for CI is potentially viable.

How AI Mitigates

AI can mitigate vulnerabilities and threat levels to ICS and CI through AGI, state awareness, diminished dependence on risk assessment, KSSM, application of data fusion and fuzzy logic within singular purpose unconscious knowledge based systems. ICS that have state awareness will be able to compare those states with KSSM that can research knowledge bases and alert human counterparts to real time issues. Infused with data fusion knowledge bases can continue to grow making AIIC more beneficial. Bundling these concepts into ICS can be a

successful technique to produce CI systems that understand risk and have potential to mitigate the vulnerability.

How AI Improves IC

The development of AIIC backed by active defense in dynamic cyclic processes can help AI improve IC and introduce RCS. State aware AIIC provide an additional layer of defense. Incorporating a dynamic cyclic process adds another. Overall, an upgrade for defense-in-depth is accomplished. Conditions noted by KSSM and expert knowledge databases coupled with data fusion advance forensic evaluations and situation awareness occurring through active defense where TIC, NSM, IR, and TEM dictate the course of action.

Critical Findings

A test of protection ability for national critical assets occurred on September 11, 2001. Beyond that event, no incidence shows the relevance of applied improvements to the cybersecurity of CIKR. The DHS and corporate executives apply confidence to risk management techniques. These techniques are unproven against happenings similar to catastrophes such as the aforementioned. Cyberweapons are a real and persistent threat to CIKR. Nation-states have and will sponsor the use of these abilities against their adversaries. Protection of CIKR is dependent upon the business attribute of risk management—an unproven idea. Several incidents record the potential of catastrophe. Partnership efforts established by DHS show little promise or real contribution. Interdependencies in CIKR sectors indicate their vitality for society and the cascading effect of disaster.

The network infrastructures of ICS's are reachable via the Internet. The protections used for standard IT infrastructures do not parallel these systems. Needs exist to reduced remote access abilities and develop advanced security for CI. OLE used to maintain CIKR industry is

dated and has not advanced security with the comprehension of the interconnected aspirations of executive decision makers.

Experts and technical minds educated in the field of PLC's and ICS's do not have the crossover knowledge to apply Internet security controls for CIKR. The same is relevant to cybersecurity experts who understand the vulnerabilities associated with the domain of cyber but do not fully realize the inability to secure ICS's. Changes in configurations and set point programming without methodical planning, testing, and only then execution result in damage, destruction, loss of product or service, and or life. Sole human dependency elevates the risk to ICS's in their interconnected characteristics. This indicates a need for advanced security in IC.

Integrating resiliency into these systems may be accomplishable through AI. While AI has not advanced to a level of conscious cognitive ability, the unconscious aspects of AI retain potential. Physical tools operating with state awareness on expert knowledge databases can achieve beneficial security applications. Physical static tools alone cannot offer absolute resiliency however. Developing information security applications for CIKR through AIIC development in conjunction with dynamic cyclic processes should prove beneficial. The premises of domain specific knowledge bases, fuzzy logic, data fusion, state awareness, situational awareness, and KSSM can potentially achieve AIIC's in active defense postures.

Future Research and Recommendations

Redirected Mitigation

Dissolving the full partnership methodology for CIKR protection is not necessary. The compiled research suggests that NIPP infuse mandated oversight and better incentive programs to assist in creation of fusion centers and knowledge bases for AIIC. Overarching cyber legislation can be detrimental but no regulation at all may create gaps for advancement of ICS's,

interdependent in nature, where failure is no option. Further recommendation contends minimizing the attack surface of CIKR can only occur with physical techniques combined with dynamic cyclic processes such as the proposed research. Dependence on the constructs of business, such as risk management, must become a secondary application. Additionally, interweaving the fields of computer programming and programmable logic is crucial for development of the intricate knowledge required by ICS experts and cybersecurity experts expected to develop security for CI. The study recommends providing test environments that have the ability to simulate ICS's so efforts conducted to improve the security of these systems can be successful.

Conceiving AIIC

Future research should examine the production of systems capable of domain specific knowledge databases. Building industrial controllers that rely on unconscious AI knowledge databases to face cyberattacks is not beyond the scope of AI. Dedication to research in this area will improve ICS engineering and the security that protects CI. Further, this research recommends placing minimal reliability on the limitations of sole human ability. Those situations connected to poor decision-making or other human shortcomings will be fewer. This should not negate the importance of human interaction and the added resilience of active defense. An improved posture pulls from both static and dynamic processes. Fusing ICS's with AI will reduce system vulnerability making them less of a target. Given the attributes to sense risk, industrial controllers will be able to deliver real-time alerts on attempts at system reconfiguration. Building knowledge databases on the premises of information security whereby a system will have the ability to choose a mitigation technique and or understand improper system authentication techniques are possible.

Application of AIIC

The proposed research advocates systems integrated with AIIC's and active defense metrics. An ability to curtail the present problem in cybersecurity made relevant by the business technique of risk management is a reasonable consideration. Future research should dedicate development of physical tools for CI systems that retain state awareness. This will allow them to apply and implement ideas such as honeypots, intrusion systems, and recovery attributes. They would also be able to interact with those analysts operating within active defense strategies. Achieving platforms for CI using characteristics such as data fusion, state awareness, fuzzy logic, knowledge databases, and ideologies premised on KSSM should be a primary consideration. Linking these attributes with dynamic cyclic processes will improve the prospect of success. Developing these attributes holds the possibility of true risk mitigation for CIKR.

Questions for Future Research

There is little case information related to systems working alone to provide defensive metrics. Because of that, there is room to explore system orientated defensive applications. Dedicating such systems to achieving analysis and mitigation but with lower level programming attributes may be worth research. Conceiving a system of this nature should not just be an isolated expenditure to CI. One such question might be: Can systems dedicated to defense apply security for connected systems? Another consideration is exploring AI concepts for other networked systems. Any progress made with CI suggests such concepts should improve defensive postures for other networked architectures. Posing the question might be: What can AI do for non-industrial networks? Finally, since this research found such a strong forbearance on active defense the question needing examination is: What advances will allow system architectures to become active defenders?

References

- Al-Askandrani, F., Amos, E., Beckman, J., Boreddy, N., Curnett, B., Martinez, C., . . . Liles, S. (2013). *Invisible attacks: Maritime shipping critical infrastructure attacks*. Center for Education and Research. West Lafayette, IN: Purdue University. Retrieved March 31, 2014, from <https://www.cerias.purdue.edu/assets/pdf/.../2013-8.pdf>
- Alexander, D. (2011, October 24). SCADA Security and the Broken Business Model for Software Testing. Tofino Security . Retrieved April 17, 2014, from <http://www.tofinosecurity.com/blog/scada-security-and-broken-business-model-software-testing>
- Auerswald, P. E., Branscomb, L. M., LaPorte, T. M., Michel-Kerjan, E. O., Apt, J., Bowe, T., & al, e. (2006). *Seeds of Disaster, Roots of Response How Private Action Can Reduce Public Vulnerability*. Cambridge, New York: Cambridge University Press. Retrieved September 9, 2014
- BCS. (2013, March 10). *Too many PCs are still running Windows XP*. (BCS, Producer) Retrieved March 10, 2014, from BCS: <http://www.bcs.org/content/conWebDoc/51393>
- Bejtlich, R. (2014). Strategy, Not Speed What Today's Digital Defenders Must Learn From Cybersecurity's Early Thinkers. Center for 21st Century Security and Intelligence at Brookings. Retrieved April 26, 2015, from <http://www.brookings.edu/~media/research/files/papers/2014/05/07-strategy-not-speed-digital-defenders-early-cybersecurity-thinkers-bejtlich/voices-from-the-cyber-past-final.pdf>
- Bommersbach, J. (2006, March). The Flight of Phoenix. Retrieved February 26, 2014, from <http://www.janabommersbach.com/pm-fea-mar06.php>

- Bologna, S., Fasani, A., & Martellini, M. (2013). *The Importance Of Securing Industrial Control Systems Of Critical Infrastructures*. General Secretariat. Como, Italy: Landau Network. Retrieved January 14, 2014, from http://www.nonproliferation.eu/documents/other/sandrobolognaalessandrofasanimaurizio_martellini516291dea8ac8.pdf
- Brecht, D. (2015). *Cyber Warfare and Cyber Weapons, a Real and Growing Threat*. Infosec Institute. Incident Response. Retrieved May 6, 2015 from <http://resources.infosecinstitute.com/cyber-warfare-cyber-weapons-real-growing-threat/>
- BusinessDictionary.com. (2014). *data fusion*. (WebFinance, Inc.) Retrieved September 20, 2014, from BusinessDictionary.com: <http://www.businessdictionary.com/definition/data-fusion.html>
- Byrnes, E., Franz, M., Carter, J., & Peterson, D. (2007). *OPC Security Whitepaper #3 Hardening Guidelines for OPC Hosts*. Lantzville, BC: Byres Research. Retrieved from www.byressecurity.com
- Carroll, D. (1966). *On the Structure of Operational Control Systems*. Massachusetts Institute of Technology. Cambridge, Massachusetts: Department of Defense. Retrieved April 14, 2014, from <http://dspace.mit.edu/bitstream/handle/1721.1/48633/onstructureofope00carr.pdf?sequence=1>
- Cavnar, B. (2010). *Disaster on the Horizon*. White River Junction, Vermont: Chelsea Green Publishing. Retrieved April 01, 2014

- Chairman of the Joint Chief of Staff. (2012). *Cyber Incident Handling Program*. Joint Chiefs of Staff. Retrieved July 26, 2014, from http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf
- Chukwu, C. (2011, June 29). *Overcoming the problems with artificial intelligence*. (C. D. LLC, Producer) Retrieved March 12, 2014, from Examiner.com: <http://www.examiner.com/article/overcoming-the-problems-with-artificial-intelligence>
- City of Tacoma. (2014). SCADA Network & Cyber Security Engineer. Retrieved December 19, 2014, from Tacoma Job Bulletins: http://agency.governmentjobs.com/tacoma/job_bulletin.cfm?JobID=940752
- Clarke, G. (2013, October 1). *500 MEELLION PCs still run Windows XP. How did we get here?* Retrieved March 10, 2014, from The Register: http://www.theregister.co.uk/2013/10/01/six_months_end_xp_support/?page=2
- Clayton, M. (2014, January 14). *Cyberexperts: a 'lost decade' since 9/11 to address infrastructure threats*. (T. C. Monitor, Producer) Retrieved February 17, 2014, from The Christian Science Monitor: <http://www.csmonitor.com/USA/2014/0117/Cyberexperts-a-lost-decade-since-9-11-to-address-infrastructure-threats>
- CCS. (2014). *How to Upgrade*. (CSS-Inc.) Retrieved March 31, 2014, from <http://www.ccs-inc.com/xp/how-to-upgrade>
- Cowan, C., Wagle, P., Pu, C., Beattie, S., & Walpole, J. (2000). Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade. DARPA Information Survivability Conference and Exposition, 2, 119-129. doi:doi: 10.1109/DISCEX.2000.821514

Davis, J. (2014, August 31). *Effects of Cyberattack Loss*. Charleston, South Carolina. Retrieved August 31, 2014

Davis, J. (2104, September 21). *Electric Turbine Cyberattack*. Charleston, South Carolina. Retrieved September 21, 2014

Davis, J. (2014, October 10). *Cyberattack Loss Equation*. Charleston, South Carolina. Retrieved October 10, 2014

Dingle, N. (2011, November 4). *Artificial Intelligence: Fuzzy Logic Explained*. Retrieved October 6, 2014, from Control Engineering: <http://www.controleng.com/single-article/artificial-intelligence-fuzzy-logic-explained/8f3478c13384a2771ddb7e93a2b6243d.html>

Exec. Order No. 13636. (2013, February 19). Executive Order No. 13636 33 F.R. 78. National Archives and Records Administration. Retrieved March 19, 2014, from <http://www.archives.gov/federal-register/executive-orders/2013.html>

Fergus, D. (2009). *Industrial Control System Security Current Trends & Risk Mitigation*. Sterling, VA: Intekras, Inc. Retrieved April 17, 2014, from www.intekras.com

Ferguson, P. (2012). *Toward a More Secure Posture for Industrial Control System Networks*. Trend Micro Inc. Cupertino, CA. Trend Micro. Retrieved January 15, 2014, from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_secure-posture-for-industrial-control-system-networks.pdf

Fischer, E. A. (2013). *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*. Congressional Research Service. Retrieved March 25, 2014, from www.fas.org/sgp/crs/natsec/R42114.pdf

- Flammini, F., Gaglione, A., Mazzocca, N., Moscato, V., & Pragliola, C. (2008). Wireless Sensor Data Fusion for Critical Infrastructure Security. *Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISIS'08, ASC 53*, p. 92. Retrieved July 16, 2014, from <https://www.docenti.unina.it/downloadP>.
- Frei, S. (2013). *Vulnerability Threat Trends*. NSS Labs. Austin, TX: NSS Labs, Inc. Retrieved January 20, 2014, from <https://www.nsslabs.com/reports/vulnerability-threat-trends>
- F-Secure. (2014). *Threat Report H2 2013*. F-Secure Corporation. Retrieved March 31, 2014, from http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H2_2013.pdf
- Genge, B., Siarerlis, C., & Karopoulos, G. (2013, June 24). Data Fusion-Based Anomaly Detection in Networked Critical Infrastructures. *Proceedings of the Seventh European Workshop on System Security*, 1-8. Retrieved September 30, 2014, from <http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=C4AFA9703A1977A98BA4489D55A5D67F?doi=10.1.1.389.6226&rep=rep1&type=pdf>
- Gerlenter, D. (2007, July 1). *Artificial Intelligence Is Lost in the Woods*. Retrieved August 3, 2014, from MIT Technology Review: <http://www.technologyreview.com/article/408171/artificial-intelligence-is-lost-in-the-woods/>
- Grinnell, F. (2009, January 9). Intelligent Design or Intelligible Design? *The Chronicle Review*. Retrieved August 3, 2014, from <http://www4.utsouthwestern.edu/frederickgrinnell/GrinnellWebMisc/intelligible%20design.pdf>

- Godreau, R. (2013). *Scada Systems And Their Vulnerabilities Within The Smart Grid: Can They Be Defended From A Cyber Attack*. Utica College, Economic Crime and Justice Studies. Ann Arbor, MI: UMI Dissertation Publishing. Retrieved March 17, 2014
- Hayes-Roth, F. (1981). *AI for Systems Management*. Santa Monica, California: The Rand Corporation.
- Harwood, M. (2012, July 6). *DHS Doesn't Know Why CIKR Stakeholders Don't*. (I. ASIS International, Producer) Retrieved April 1, 2014, from Security Management: <http://www.securitymanagement.com/news/dhs-doesnt-know-why-cikr-stakeholders-dont-participate-voluntary-security-assessments-0010059?page=0%2C1>
- Hayes, B. (2012). The Manifest Destiny of Artificial Intelligence. *American Scientist*, 100. Retrieved August 3, 2014, from <http://www.americanscientist.org/libraries/documents/2012612149269144-2012-07Hayes.pdf>
- Higgins, K. (2013, August 1). *SCADA Experts Simulate 'Catastrophic' Attack*. (UBM Tech) Retrieved January 20, 2014, from Dark Reading: <http://www.darkreading.com/attacks-breaches/scada-experts-simulate-catastrophic-atta/240159333>
- Horvitz, E. (1996, August). Decisions, Uncertainty and Intelligence. *Proceedings of AAAI-96*. Portland, Oregon: AAAI Press. Retrieved January 27, 2014, from <http://research.microsoft.com/en-us/um/people/horvitz/seltext.htm>
- Honeywell. (2014). *Effective Use of Assessments for Cyber Security Risk Mitigation*. Houston, TX: Honeywell International, Inc. Retrieved March 25, 2014, from <https://www.honeywellprocess.com/library/marketing/whitepapers/White-Paper-Effective-Use-of-Assessments-for-Cyber-Security-Risk-Mitigation.pdf>
- Huler, S. (2010). *On The Grid*. New York, New York: Rodale. Retrieved April 1, 2014

ICS-CERT. (2013). *ICS-CERT Monitor*. United States Department of Homeland Security. ICS-CERT. Retrieved January 20, 2014, from http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monitor_April-June2013.pdf

ICS-CERT. (2014). *ICS-CERT Monitor*. United States Department of Homeland Security. Retrieved September 21, 2014, from https://ics-cert.us-cert.gov/sites/default/files/monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf

Informatica. (2013). *Data Fusion for Cyber Intelligence*. Redwood City, CA: Informatica Corporation. Retrieved July 26, 2014, from http://www.federalnewsradio.com/pdfs/InformaticaData-fusion-cyber-intelligence_eb_en-US.pdf

InfraGard. (2014). *Emergency Services Sector*. (InfraGard San Diego Members Alliance) Retrieved September 20, 2014, from InfraGard San Diego: <http://www.infragardsd.org/sector-emergency.html>

International Group of Experts. (2013). *Tallin Manual On The International Law Applicable to Cyber Warfare*. Michael N. Schmitt. Cambridge University Press. Retrieved May 10, 2015 from https://archive.org/stream/TallinnManual/TallinnManual_djvu.txt

Jacobs, M. (2013, February). *Bob Lockhart, Tofino Security: SCADA Security: Big Picture Planning is Key*. (Global Security Mag) Retrieved April 17, 2014, from Global Security Mag: <http://www.globalsecuritymag.fr/Bob-Lockhart-Tofino-SCADA-Security,20130218,35498.html>

Johnson, R. C. (2013, October 28). *Vicarious AI Passes Turing Test*. (UBM Tech) Retrieved August 3, 2014, from EE Times: http://www.eetimes.com/document.asp?doc_id=1319914

- Juniper Networks. (2010). *Control System Cyber Vulnerabilities and Potential Mitigation of Risk for Utilities*. Sunnyvale, CA: Juniper Networks, Inc. Retrieved March 18, 2014, from www.juniper.net/us/en/local/pdf/.../2000267-en.pdf
- Kaplan, J., Sharma, S., & Weinberg, A. (2011, June). Meeting the cybersecurity challenge. *McKinsey & Company*. McKinsey & Company. Retrieved April 17, 2014, from http://www.mckinsey.com/insights/business_technology/meeting_the_cybersecurity_challenge
- Keller, J. (2013, March 26). *DARPA launches PPAML artificial intelligence program to move machine learning forward*. Retrieved August 3, 2014, from Military Aerospace: <http://www.militaryaerospace.com/articles/2013/03/DARPA-machine-learning.html>
- Kerr, D. (2013, January 24). 'Cyber 9/11' may be on horizon, Homeland Security chief warns. (C. I. Inc., Producer) Retrieved 28 2014, February, from CNET: http://news.cnet.com/8301-1009_3-57565763-83/cyber-9-11-may-be-on-horizon-homeland-security-chief-warns/
- Langner, R., & Pederson, P. (2013, February). Bound to Fail: Why Cyber Security Cannot Be "Managed" Away. *Center for 21st Century Security and Intelligence*. Retrieved June 10, 2014, from http://www.brookings.edu/~media/research/files/papers/2013/02/cyber%20security%20langner%20pederson/cybersecurity_langner_pederson_0225.pdf (Langner & Pederson, 2013)
- Lee, R. M. (2015). Active Cyber Defense Cycle. Keynote Address for BSides. Retrieved April 20, 2015, from <http://www.irongeek.com/i.php?page=videos/bsides huntsville2015/active-cyber-defense-cycle-robert-m-lee>

- Leverett, E. P. (2011). *Quantitatively Assessing and Visualising Industrial System Attack Surfaces*. Darwin College, Computer Laboratory. University of Cambridge. Retrieved March 27, 2014, from <https://www.google.com/webhp#q=Attack+Surface+of+Industrial+Controllers>
- Lewis, H. W. (1997). *The Foundations of Fuzzy Control*. New York, NY: Plenum Press. Retrieved October 1, 2014
- Lieberman, P. (2012, March). *Security Management: The Scary New Hacking Trend*. (Microsoft) Retrieved April 16, 2014, from TechNet Magazine: <http://technet.microsoft.com/en-us/magazine/hh859722.aspx>
- Linda, O., Manic, M., & McQueen, M. (2012). *Improving Control System Cyber-State Awareness Using Known Secure Sensor Measurements*. Idaho National Laboratory. Retrieved September 30, 2014, from <http://www.inl.gov/technicalpublications/Documents/5517258.pdf>
- Loney, M. (2004, March 1). *US software 'blew up Russian gas pipeline'*. (CBS Interactive) Retrieved February 27, 2014, from ZDNet: <http://www.zdnet.com/us-software-blew-up-russian-gas-pipeline-3039147917/>
- Lusignea, M. (2013, July 16). *Cyber Security, Beyond the Internet: An Automation Engineer's View*. (exida.com LLC) Retrieved April 16, 2014, from exida: http://exida.com/Blog/cyber_security_beyond_the_internet_an_automation_engineers_view
- Luth, J. (2004, December 28). *Unified architecture – The future of OPC*. (Control Global) Retrieved January 22, 2014, from Control: <http://www.controlglobal.com/articles/2004/229/>

- Lynch, G. (2012, December 1). *Are Industrial Control Networks Secure?* (Industrial Control Systems Engineering) Retrieved April 15, 2014, from Industrial Control Systems Engineering: <http://www.icsenggroup.com/are-industrial-control-networks-secure/>
- Massaro, S. (2008, May 15). What is OPC UA and how does it affect your world? (Control Engineering). Plant Engineering. Retrieved January 21, 2014, from http://www.plantengineering.com/index.php?id=1792&cHash=081010&tx_ttnews%5Btt_news%5D=35007
- Matrosov, A., Rodionov, E., Harley, D., & Malcho, J. (2011). *Stuxnet Under the Microscope*. Eset North America. Retrieved January 20, 2014, from http://www.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf
- McCusker, R. (2006). Transnational organised crime: distinguishing threat from reality. *Crime, Law and Social Change*, 46(4-5), 257-273.
- Mello, J. (2013a, September 26). *Spear phishing poses threat to industrial control systems*. (CXO Media Inc.) Retrieved January 20, 2014, from CSO: <http://www.csoonline.com/article/740396/spear-phishing-poses-threat-to-industrial-control-systems>
- Mello, J. (2013b, August 20). *Study finds big gap about app security between execs and IT staffers*. (C. M. Inc., Producer) Retrieved March 13, 2014, from CSO: <http://www.csoonline.com/article/738490/study-finds-big-gap-about-app-security-between-exec-and-it-staffers>
- Mick, J. (2011, April 28). U.S. Gov't Study: Over a Third of FBI Cyber-Crime Agents are Incompetent. Daily Tech L.L.C. Retrieved September 7, 2014, from <http://www.dailytech.com/US+Govt+Study+Over+a+Third+of+FBI+CyberCrime+Agents+are+Incompetent/article21490.htm>

- Moore, T. (2010). *Introducing the Economics of Cybersecurity: Principles and Policy Options. Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*. Retrieved April 16, 2014, from <http://www.nap.edu/catalog/12997.html>
- Moravec, H. (2009, March 23). *Artificial Intelligence*. (S. American, Producer) Retrieved September 22, 2014, from *Scientific American*: <http://www.scientificamerican.com/article/rise-of-the-robots/>
- Mueller, P., & Yadegari, B. (2012). *The Stuxnet Worm*. University of Arizona, Department of Computer Science. Retrieved March 27, 2014, from <http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf>.
- Nakashima, E., & Warrick, J. (2012, June 2). *Stuxnet was work of U.S. and Israeli experts officials say*. Retrieved from *The Washington Post*: http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html
- National Security Agency. (2010). *A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS)*. National Security Agency of The United States of America, Systems and Network Analysis Center. Systems and Network Analysis Center NSA. Retrieved January 15, 2014, from http://www.nsa.gov/ia/_files/ics/ics_fact_sheet.pdf
- NATO Science for Peace and Security Series. (2008). *Responses to Cyber Terrorism* (Vol. 34). (C. o. D. Terrorism, Ed.) Ankara, Turkey: IOS Press.

- Nilsson, N. J. (2010). *The Quest For Artificial Intelligence*. Cambridge, UK: Cambridge University Press. Retrieved September 23, 2014, from <http://ai.stanford.edu/~nilsson/QAI/qai.pdf>
- Paine, T. (2008, July 1). *Meet the Next Generation of OPC*. (Questex Media Group, LLC) Retrieved January 23, 2014, from Sensors: <http://www.sensorsmag.com/networking-communications/industrial-networking/meet-next-generation-opc-1494>
- Parfomak, P. W. (2014). *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*. Congressional Research Service. Retrieved September 19, 2014, from <http://fas.org/sgp/crs/homesec/R43604.pdf>
- Peterson, D. G. (2011, March 21). *Italian Researcher Publishes 34 ICS Vulnerabilities*. (Digital Bond, Inc.) Retrieved February 17, 2014, from Digital Bond: <http://www.digitalbond.com/blog/2011/03/21/italian-researcher-publishes-34-ics-vulnerabilities/>
- Ramzy, A. (2014, March 9). *China Warns of Risks in Plan to Retire Windows XP*. (T. N. Company, Producer) Retrieved March 31, 2014, from The New York Times: http://sinosphere.blogs.nytimes.com/2014/03/09/china-warns-of-risks-in-plan-to-retire-windows-xp/?_php=true&_type=blogs&_r=0
- Rawat, M. (2014, February 4). *Buffer Overflow Basics*. (I. Institute, Producer) Retrieved September 16, 2014, from InfoSec Institute: <http://resources.infosecinstitute.com/buffer-overflow-basics/>
- Renaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001, December). Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control System's Magazine*. Retrieved April 1, 2014, from [http:// user.it.uu.se/~bc/Art.pdf](http://user.it.uu.se/~bc/Art.pdf)

- Rieger, C. G., Gertman, D. I., & McQueen, M. A. (2009). *Resilient Control Systems: Next Generation Design Research*. Catania, Italy: Idaho National Laboratory. Retrieved July 4, 2014, from <http://www.inl.gov/icis/controlsystems/resilient-control-systems.pdf>
- Roulo, C. (2014, February 27). Alexander: Laws, Policies Lag Behind Changes in Cyber Threats. *US Department of Defense*. Washington, DC, USA: American Forces Press Service. Retrieved March 25, 2014, from <http://www.defense.gov/news/newsarticle.aspx?id=121745>
- Russell, S., & Norvig, P. (2010). *Artificial Intelligence* (Third Edition ed.). Upper Saddle River, New Jersey 07458: Pearson Education, Inc. Retrieved June 27, 2014
- Salamon, A., Rayhawk, S., & Kramar, J. (2010). How Intelligible is Intelligence? (K. Mainzer, Ed.) *ECAP10: VIII European Conference on Computing and Philosophy*. Retrieved August 3, 2014, from <https://intelligence.org/files/HowIntelligible.pdf>
- Sammet, J. E. (1971). *Challenge to Artificial Intelligence: Programming Problems to be Solved*. London: Second International Joint Conference on Artificial Intelligence. Retrieved January 27, 2014, from <http://www.ijcai.org/Past%20Proceedings/IJCAI-1971/PDF/005%20C.pdf>
- Sanders, D. (2013, October 30). *Artificial intelligence tools can aid sensor systems*. Retrieved October 6, 2014, from Control Engineering: http://www.controleng.com/single-article/artificial-intelligence-tools-can-aid-sensor-systems/4c5c55d7e7e60c54f8efa6c363302ac9.html?tx_ttnews%5BViewItem%5D=3
- SCADAhacker. (2014). *Library of Resources for Industrial Control System Cyber Security*. Retrieved November 8, 2014 from <http://scadahacker.com/library/>.

- Shea, D. (2003). *Critical Infrastructure*. The Library of Congress. Congressional Research Service. Retrieved January 14, 2014, from <http://www.fas.org/irp/crs/RL31534.pdf>
- Shook, S. (2014, March 28). *To XP or Not to XP*. (C. Inc., Producer) Retrieved September 17, 2014, from Cylance: <http://blog.cylance.com/to-xp-or-not-to-xp>
- Simon, H. A., & Newell, A. (1964). *Hueristic Problem Solving By Computer*. Computer Science Department. Allen Newell Collection. Retrieved January 28, 2014, from <http://digitalcollections.library.cmu.edu/portal/service.jsp?awdid=16&smd=1#>
- Smith, R. (2014, March 12). U.S. Risks National Blackout From Small-Scale Attack. *The Wall Street Journal*. Dow Jones & Company, Inc. Retrieved September 19, 2014, from <http://online.wsj.com/news/articles/SB10001424052702304020104579433670284061220>
- Sowa, J. F. (2002). Architectures for Intelligent Systems. *IBM Systems Journal*, 41(3), pp. 331-349. Retrieved August 3, 2014, from <http://www.jfsowa.com/pubs/arch.htm>
- Stouffer, K., Falco, J., & Kent, K. (2006). *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Systems*. NIST Special Publication. Department of Commerce. Retrieved March 27, 2014, from <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCkQFjAA&url=http%3A%2F%2Fwww.dhs.gov%2Fsites%2Fdefault%2Ffiles%2Fpublications%2Fcsd-nist-guidetosupervisoryanddataacquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf&ei=K>
- Spiegel, R. (2008, September 1). *Building from Worker to the Queen*. (Summit Media Group, Inc.) Retrieved January 21, 2014, from Automation World: <http://www.automationworld.com/information-management/building-worker-queen>

- The Information Assurance Directorate. (2002, September 1). *Defense in Depth*. Retrieved January 16, 2014, from IAD:
<https://www.iad.gov/iad/documents.cfm?zBI+E5+sBQ8l785Hms9M3TTGZMqX89HtgARktF8oEX0=>
- The Archive. (2013, April 26). Update: Agent Farewell and the Siberian Pipeline Explosion. *Unredacted*. Retrieved February 17, 2014, from
<http://nsarchive.wordpress.com/2013/04/26/agent-farewell-and-the-siberian-pipeline-explosion/>
- Tofino. (2013). *Tofino Live Demonstration*. (Tofino) Retrieved April 17, 2014, from Tofino:
<http://www.tofinosecurity.com/VideoSummary/TofinoLiveDemonstration>
- Udassin, E. (2008). *Control System Attack Vectors and Examples: Field Site and Corporate Network*. Ramat, Israel: C4 Security. Retrieved February 17, 2014, from <http://www.c4-security.com/SCADA%20Security%20-%20Attack%20Vectors.pdf>
- US Department of Homeland Security. (2010). *Critical Infrastructure & Key Resources*. Science and Technology Directorate. Washington, DC: US Department of Homeland Security. Retrieved April 1, 2014, from
http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=5&ved=0CEwQFjAE&url=http%3A%2F%2Fwww.dhs.gov%2Fxlibrary%2Fassets%2Fst_cikr_requirements_book_jan_2010.pdf&ei=0iY7U8yDJvHQsQSw5IDwCw&usg=AFQjCNGfvM7eorzZtFX93chowJVfNtIZpQ&sig2=j9hp09bi_6M6
- US Department of Homeland Security. (2011). *Buildings and Infrastructure Protection Series*. US Department of Homeland Security, Science and Technology Directorate. Retrieved March 31, 2014, from www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf

- US Government Accountability Office. (2011, July). Defense Department Cyber Efforts. *GAO Report to Congressional Requesters(GAO 11-75)*. Retrieved September 7, 2014, from <http://www.gao.gov/new.items/d1175.pdf>
- Voss, P. (2002). *Essentials of General Intelligence: The direct path to AGI*. Retrieved August 3, 2014, from Adaptive A.I. Inc.: <http://adaptiveai.com/research/>
- Wald, M. L. (2013, November 14). *Attack Ravages Power Grid. (Just a Test.)*. (T. N. Company, Producer) Retrieved February 27, 2014, from The New York Times: http://www.nytimes.com/2013/11/15/us/coast-to-coast-simulating-onslaught-against-power-grid.html?_r=0&adxnnl=1&smid=tw-nytimes&adxnnlx=1384501226-AiLoSrpp3l0LspF4Ovg/hw
- Yang, Y., & Syndor, R. (n.d.). *Resilient Control for Critical Infrastructures and Systems*. Office of Research. US Nuclear Regulatory Commission. Retrieved July 4, 2014, from <http://pbadupws.nrc.gov/docs/ML1214/ML12144A058.pdf>
- Zatarain, A. (2005, March). *Outwit Control System Gremlins*. Putnam Media. Retrieved January 23, 2014, from http://www.artzat.com/pubs/amz_reliability_2005.pdf
- Zatarain, A. M. (2014, March 9). personal communication. Retrieved March 10, 2014
- Zatarain, A. M. (2015, June 7). personal communication. Retrieved June 7, 2015
- Zwan, E. v. (2010). JOnline: Security of Industrial Control Systems. *ISACA Journal*, 4. Retrieved September 21, 2014, from ISACA: <http://www.isaca.org/Journal/Past-Issues/2010/Volume-4/Documents/10v4-online-security-of.pdf>

Appendices

Appendix A- Hacking or Disruption to SCADA

A Short Chronological List of Widely Reported Incidents of Hacking and Disruption	
Feb 2009	Highly evasive Conficker/Downadup worm infects 12 million computers, stealing information. - BBC
Jun 2008	"Security Hole Exposes Utilities to Internet Attack" - Associated Press
May 2008	SCADA vulnerability...control software used by one-third of industrial plants. - SC Magazine
Mar 2008	Emergency 2-day shutdown of Hatch nuclear plant from software update on one business computer.
Feb 2008	Retail Chinese digital picture frame virus steals passwords and financial info. - SF Chronicle
Jan 2008	Hackers turn out the lights in multiple cities and demand extortion payments." - Associated Press
Sep 2007	DOE Idaho National Lab video shows the remote destruction of a large SCADA controlled generator.
Sep 2007	Hackers compromise Homeland Security computers, moving information to Chinese websites. - CNN
Jul 2007	3Com's security division demonstrates how SCADA system flaws can be exploited.
Nov 2007	"Insider Charged with Hacking California Canal System" - ComputerWorld
Nov 2007	"Solar Sunrise" - Three teenagers penetrate USAF logistic systems at Middle East support bases.
Aug 2007	"Hackers Take Down the Most Wired Country in Europe" for two weeks. - Wired Magazine
Jun 2006	"Information on SCADA systems can be found by a determined attacker." - US-CERT
Jan 2006	Homeland Security Conference - SCADA systems are vulnerable to intrusion. - UrgentComm
Jan 2006	"SCADA Security & Terrorism: We're Not Crying Wolf" conference presentation. - Xforce Security
Aug 2005	175 companies including Caterpillar, General Electric, UPS and DaimlerChrysler attacked by Zotob worm.
2003-2005	Undetected for 2 years, Chinese Army downloads 10-20 terabytes data from Pentagon, DOE, others.
Aug 2003	CSX loses signaling & dispatch control over 23 state railroad due to a worm virus. - InformationWeek
2003	"Cyber War" - PBS Frontline documents penetration of US utilities using commonly known methods.
Jan 2003	Davis-Besse nuclear plant safety monitoring system knocked offline 5-hours by the Slammer worm.
Jan 2003	"Slammer" worm infects 300,000 computers in the first 15 minutes, interrupting 911 and airlines.
Sep 2001	"Nimda" worm infects millions of computers causing billions of dollars in damage. Originator unknown.
Jul 2001	"Code Red" worm infects 300,000 computers in a month and then launches an attack on White House web.
Apr 2000	Hackers succeeded in gaining control of the world's largest natural gas pipeline network (GAZPROM).
Apr 2000	Hacker uses a SCADA system to dump millions of gallons of sewage onto hotel grounds for 3 months.
1998-2000	"Moonlight Maze" - For two years, hackers penetrated the Pentagon, NASA, DOE, university research labs.
1998	A 12-year-old hacks into Roosevelt Dam, with complete SCADA system control of massive floodgates.
1997	"Eligible Receiver" - DOD & Joint Chief Command hacked in 48 hours with publicly available methods.
1997	A teenager hacks into NYNEX and cuts off air/ground communication to Worcester Airport for 6 hours.
	Many more incidents go unreported for reasons of national security or corporate embarrassment. Even more go undetected. Properly executed, successful hacks are undetectable and untraceable.

Note. By Hacking the Industrial SCADA Network (Dickman, 2009).

Appendix B- List of Abbreviations

ACDC- Active Cyber Defense Cycle

AI- Artificial Intelligence

AIIC- Artificially Intelligent Industrial Controllers

A&E- Alarm & Event

AGI- Artificial General Intelligence

ASI- Artificial Security Intelligence

ASP- Active Server Page

CI- Critical Infrastructure

CIKR- Critical Infrastructure and Key Resources

COM- Component Object Model

COTS- Commercial of the Shelf

CRC- Cyclic Redundancy Checking

DA- Data Access

DCOM- Distributed Component Object Model

DHS- Department of Homeland Security

DMZ- Demarcation Zone

EO- Executive Order

ESS- Emergency Services Sector

GAO- Government Accountability Office

IA- Information Assurance

IC- Industrial Controller

ICN- Industrial Control Network

ICS- Industrial Control System

ICS-CERT- The Industrial Control Systems Cyber Emergency Response Team

IR- Incident Response

KSSM- Known Secure Sensor Measurement

NERC- The North American Electric Reliability Council

NIPP- The National Infrastructure Protection Plan

NSA- National Security Agency

NSM – Network Security Monitoring

OLE- Object Linking and Embedding

OPC- Object Linking and Embedding for Process Control

OPC-UA- Object Linking and Embedding for Process Control-Unified Architecture

OS- Operating System

POS- Point of Sale

RCS- Resilient Control System

SCADA- Supervisory Control and Data Acquisition

SOA- Service Oriented Architecture

TCP/IP- Transmission Control Protocol/Internet Protocol

TEM- Threat Environment Manipulation

TIC- Threat Intelligence Consumption

TTP- Tactics, Techniques, and Procedure