CREATING REALISTIC CYBERSECURITY POLICIES FOR INDUSTRIAL CONTROL SYSTEMS

David Blanco
SCADA Security Adviser
Automation Solutions, INC.
16055 Space Center Blvd, Suite 450
Houston, TX United States of America

January 20, 2017

Introduction

As the airplane added the skies to the battlefields of WW1 and the Cold War launched confrontations into space, Stuxnet has pushed the boundaries of war and politics into cyberspace. Now anything with an internet connection can be the target of an attack. While this might be ignored as something primarily affecting the Internet of Things (IoT), it's prudent to point out those industrial control systems (ICS) and their supervisory control and data acquisition (SCADA) networks have been functioning as an industrial IoT before there was an Internet. Today's SCADA networks have adopted new technologies that allow data and commands to pass quickly between the most remote field site and the control room. It's true that this enhances the safety and profitability of a system, but it's also true that the cutting edge is often double-edged.

Equipping SCADA networks with the capability of real-time command and control enhanced process safety, but created network insecurity. The protocols and networking hardware used to communicate between the office and remote sites are a mish-mash of company practices, financial realities, and acquisitions that create opportunities for exploitation. Since the availability of data is a SCADA department's priority, if the data comes in, everyone is happy. However, hostile actors now have the ability to manipulate data, take over field equipment, and destroy property as well as lives because of exploits hidden into the structure of SCADA networks and hardware. Supporting this is the fact that attacks on SCADA networks more than doubled in 2016.[1] Those who attempted to address this have turned to their IT departments, hardware vendors, as well as government and industry guidelines, but this often creates conflicts, complexity, and confusion. Cybersecurity is not a binary process, it's a relative, cumulative, and flexible process. Just like SCADA networks, cyber solutions are diverse since no one vendor, product, or service can protect an environment from every attacker.[2] Ultimately, the security of SCADA networks is up to SCADA departments.

SCADA departments have the technical and process knowledge to successfully foster a secure environment without impeding business. It's also true that SCADA departments are the ones held accountable, criminally and professionally, for the safety of the systems they operate. Within the context of SCADA, cybersecurity shares the same goal as SCADA departments: safety. When a SCADA network is secure it has the opportunity to operate safely. For these reasons, SCADA departments must begin creating their own cybersecurity policies. That's not to say they have to operate in conflict with IT, but the operational differences between SCADA and IT leave IT impotent at the field level and force SCADA to take responsibility. Therefore, SCADA departments must create their own cybersecurity policies that balance safety goals with business goals. This paper will help SCADA do that by addressing the challenges this process faces and offering solutions through specific technology adoption as well as device level security policy analysis. This paper's success will be measured by how quickly its contents move from the boardroom to the test lab, to the field.

To accomplish this, the paper proceeds as follows. First, it presents examples of attacks against SCADA networks to find a baseline for discussing what makes good policy. Then it discusses how the current dynamic between SCADA and IT departments helped create the vulnerabilities hackers exploit. Afterward, it identifies the need for a SCADA cybersecurity policy by defining SCADA in a new context and outlining why SCADA would benefit from an independent cybersecurity policy. Finally, the paper outlines the goals of a SCADA cybersecurity policy, lists the technologies that can meet those goals, and outlines the most actionable security guidelines for SCADA networks to adopt.

Threats Against SCADA: Be on High High Alert

Creating and implementing a cybersecurity policy for a SCADA network is challenging work that is ultimately a project about enabling business to continue as its operating environment become more hostile. With energy prices struggling, the case for dedicating the resources needed for this task will require evidence that SCADA networks are threatened. The arguments made against taking steps to secure SCADA networks usually imply arguments like "our SCADA network *won't* get hacked." However, assuming a network is not a target is one of the biggest mistakes companies make.[3] It's impossible to prevent being attacked, but it is possible to prevent an attack from doing damage. Another argument that is often made is that SCADA *can't* be hacked. These opinions are not designed to help stakeholders create efficient cybersecurity policies for SCADA networks, rather, they're designed to shut down any discussion of security by framing the issue as improbable and impossible. This is extremely problematic since hacking SCADA networks is not only possible, but happening at an increasing rate.

Cyber-attacks against ICS networks increased by 110 percent in 2016 from their 2015 numbers.[4] Considering how every year since 2011 has seen an increase in SCADA attacks, with over 675,000 attacks occurring in 2014, it is safe to say that cyber-attacks against SCADA networks are on a strong upward trend.[5] The implication of this is

that the people and organizations doing the hacking feel that they're getting a good return on their investment, so the upward trend in SCADA attacks is likely to continue. This is true not only because North America has the most industrial devices connected to the internet, but also because new vulnerabilities are discovered for ICS equipment every year, with 189 new ones discovered last year.[6] It's also important to note that "most breaches go unnoticed or are never publicly reported."[7] A company is not required to report a hack unless the personal, financial, or medical records of individuals was compromised.[8] As industry relevant proof of this assertion, the Industrial Control System Cyber Emergency Response Team's (ICS-CERT) numbers can be investigated. ICS-CERT is a team of cybersecurity specialists working under the Department of Homeland Security that can be called into cyber-incidents to help contain and analyze an attack. ICS-CERT responded to 295 incidents in 2015, but few of those incidents can be searched for and verified successfully.[9] ICS-CERT publishes that it responded to an incident, but anonymizes the attack details before publication. While this creates a sense of urgency in the abstract, these facts don't help cybersecurity policymakers create effective policies. This is because facts without context are trivia, not truths. To whittle these assertions down to a fine enough point to write a cybersecurity policy for SCADA networks, more comprehensive examples are required that give specific proofs of the kinds of threats SCADA networks face.

In 2008, a crude oil pipeline in Turkey exploded after hackers over pressurized the line by taking control of several valves.[10] The hackers had such a grip on the system, that the control room didn't learn about the incident until 40 minutes after the explosion, because the hackers switched the alarms off for the affected site.[11] The hackers also managed to cover their tracks by deleting over 60 hours of surveillance footage of the affected site. Although both American and foreign intelligence officials asserted the attack was perpetrated by Russia, using circumstantial evidence of the motive and sophisticated means of the attack, no one seems to know who launched this attack for certain. This incident exemplifies the ultimate threat to SCADA networks, which is remote control of equipment by a hostile entity who proceeds to use the mechanics of the equipment to a malicious end. Ultimately, what this incident serves as is proof that hackers can and are trying to destroy SCADA equipment. The idea that SCADA is too niche or too difficult to hack, that SCADA can't be hacked, is completely undermined by this attack. It also shows that it's not necessary for an attacker to change the equipment for an attack to be successful, but merely to use the equipment in an unsafe manner. The implication of this is that SCADA equipment itself need not be infected to be destructive. Hackers only need access to cause damage.

In 2012, Kyle Wilhoit, a SCADA security researcher, setup three SCADA systems and put them on public American IP addresses to gauge the capabilities of SCADA hackers. After being online for only 28 days, the systems suffered 39 attacks from 11 countries.[12] Many of the attacks were from automated attack scripts, trawling the internet looking for matching IP-Port combinations of known ICS equipment. Around 12 of the attacks were sophisticated enough to be labeled "targeted." The maliciousness of the attack can be best understood by the following example. One hacker modified a pump pressure setpoint and raised a water temperature setpoint while another created a new scheduled task to shut down the pipe.[13] Mr. Wilhoit conducted this test again, but with 12 fake SCADA systems, using IP addresses from around the globe. The results were much the same. In one incident, the hacking group APT1, a branch of the Chinese army, hacked what it thought was a US water municipality causing "critical" damage to the facility.[14] The idea of securing SCADA assets by obscurity, that is hiding the location of assets and hoping the mystery behind their internal mechanisms keeps it safe, is no longer viable. If equipment is hooked up to the Internet, then there is someone looking for it with the means to manipulate it. Also, if that equipment is using a public IP address, then hackers could circumvent the IT department's protections and go straight for the field assets themselves. Even though Mr. Wilhoit's experiments used public IP addresses, there are also vulnerabilities for SCADA networks hosted over cloud services.

While there are numerous benefits to the cloud for SCADA systems like better uptime and redundancy, cybersecurity is not necessarily one of them. Employees of cloud services can access client's networks and data despite company policies against the practice as happened with Google when employees were caught violating users' privacy.[15] Companies lose control of their network when they opt for a cloud provider. Yes, the data makes it from point A to point B, but what happens to that data between these points and who else has access to the network is unknown to the end user. For example, a user's confusion over one setting on Amazon Cloud allowed one client's sales records and another client's source code to be exposed to the public.[16] Companies that choose the cloud also must trust the cloud provider to not introduce new connections to the SCADA system, either by policy or accident, since these easily create "unknown risks" for the system.[17] Some of the most common protocols, such as Modbus and DNP3 can be "easily spoofed" if SCADA is moved to the cloud, allowing an attacker to gain access to sensitive control data.[18] Basically, adding a bump in the wire between the field assets and the control stations could introduce something that goes bump in the night.

Another example of a SCADA hack came in 2015 when hackers gained access to a furnace at a German steel mill. The hackers were able to prevent a controlled shut down of the furnace, resulting in "massive damage" to the facility.[19] While the German government has not released the name of the company or specifics of the attack, what is clear is that the hackers had "extended to detailed knowledge of applied industrial controls and production processes."[20] This lends credence to the idea that this incident was the creation of a nation-state, rather than just an individual or group of private citizens. It is not entirely clear if the hackers intended to destroy the furnace or if it was an accident that happened as a domino effect of the hackers' mere presence in the system. Similarly, it is hard to ascertain why the steel mill's safety procedures failed to stop the meltdown. What this attack and the other examples indicate, is that hacking SCADA systems is primarily the business of nation states.

While it is true that some individuals and smaller organizations like terrorists and Anonymous do have the motives and in some cases the means to hack SCADA, the attacks that do the most damage and require the most preparation to execute are primarily done by state actors.[21] Nation states have the resources, the time, manpower, and money, to launch attacks that penetrate deep and persist for years. Apart from the incidents already discussed, further proof of this argument is the link between geopolitics and the hacking of ICS. Figure 1 demonstrates this point. The first big spike in SCADA attacks that took place in November 2013 is denoted by the red line. This spike coincided with President Obama's announcement that the US would begin negotiation with Iran about the latter's nuclear program.[22] The second large spike in April, 2014, as denoted by the orange line, coincides with the beginnings of very tense rounds of negotiations. The who and the why are open to speculation, but the data shows a clear link between geopolitics and targeting ICS. Another example of this idea comes from Sweden's ICS industries where "geopolitical interests" made Sweden a target of the Russian malware BlackEnergy2.[23] Luckily the malware was caught before it could do any physical damage. However, this malware did have the capability to overwrite data on the ICS and looked to be "intended for sabotage."[24]

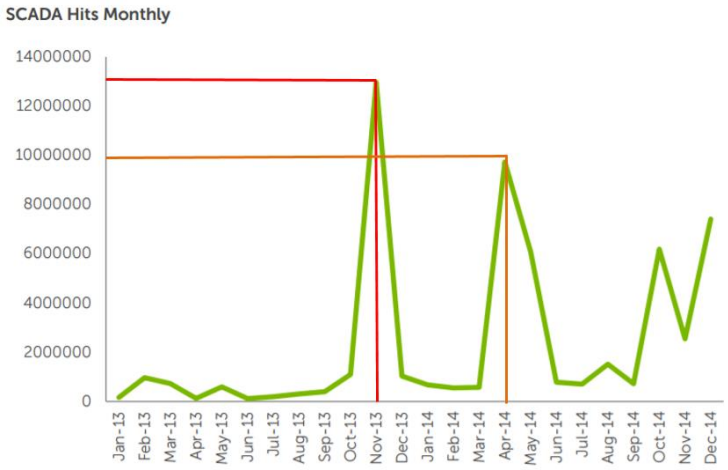

Figure 1: SCADA Hits Against US Monthly [25]

Even at this point, there may still be doubts about the ferocity of SCADA hacking. As this paper outlined earlier, the number of hacking incidents more than doubled last year, which begs the question, *why haven't there been more news stories about ICS damages?* Under-reporting can't account for all attacks, after all, if there were explosions and leaks every other month the news would certainly pick up the stories. The answer is that the ability to destroy ICS equipment is a strategic weapon. For example, a country will fly bombers at or over the territory of another country in order to gauge the reaction of the other country.[26] Did the other country scramble fighters, lock missiles on it, or track it with radar? Was the bomber even detected? Ultimately, this is preparation for war, to know what to expect when it matters. Countries will use their ability to disrupt their enemies' critical infrastructures at the most politically, economically, or militarily advantageous moment. One example of this kind of attack is Operation Cleaver. This attack was two years old when it was discovered and had penetrated several ICS networks of 50 companies in 16 countries.[27] This malware would take screenshots and log keystrokes, allowing the hackers to get deeper and deeper into the system. It would purposely target drawings of sites labeled "mission critical."[28] Luckily this malware was caught before physical damage could be done, but this kind of attack will become more common. Experts estimate that about 30 nations have acquired offensive cyber capabilities, with the skills to target ICS.[29] Several national security experts have pointed out that, "Eventually, all modern militaries will have offensive cyber capabilities."[30] While it is true, that defenses for standard hack attacks do exist, they don't exist in a form that SCADA can leverage. As Dr. Patrick Down, the Chief Architect of the NSA,

pointed out in 2013, there is an uneven distribution of cyber defenses on American networks, with some places having 100ft tall walls while others have 2ft tall walls."[31] SCADA has a 2ft wall. Working security is needed for SCADA because the frequency of attacks is not the issue, it's the consequences of the impact that matters.

SCADA Security Challenges: Function over Form

Awareness of the threats to SCADA networks helps policymakers create stronger procedures because it exposes the flaws in the current system that hackers are exploiting. Therefore, the foundation of good policy must be built on understanding the failure points in current SCADA cybersecurity policy and changing how SCADA security is approached to overcome these threats. One of the biggest failure points in SCADA cybersecurity is the belief that IT cyber solutions can address SCADA security problems. SCADA can borrow from IT, but cannot become IT. Since cyber-attacks can take advantage of processes, software flaws, hardware exploits, and human error, SCADA must be viewed as a broader process, rather than an input-output system, so that those wider elements can be taken into account when crafting a cybersecurity policy. Traditionally, a SCADA network is a system for remote monitoring and control that operates over a communication channel.[32] For the purposes of this paper, SCADA networks must also include all the hardware, software, processes, and people that are involved in moving data from the point of its generation to the point of its consumption. Consequently, where IT security ends and SCADA security begins is the first step in understanding where SCADA is vulnerable.

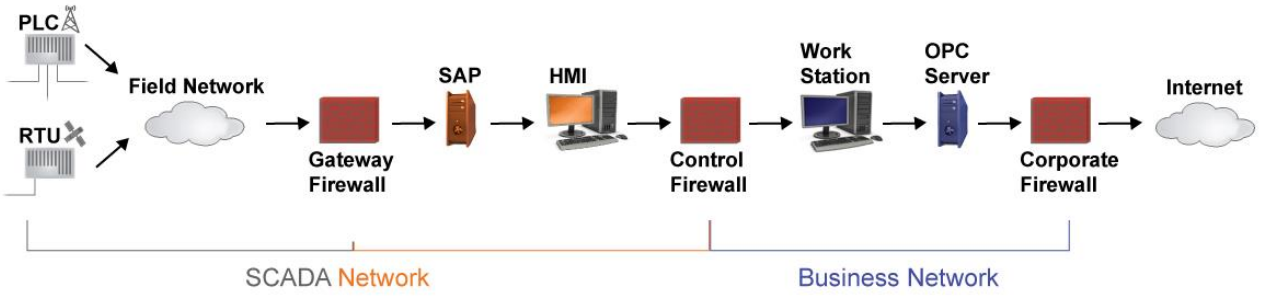

Figure 2: A Typical SCADA Network

An example of a typical SCADA network is presented above in Figure 2. Using this, a SCADA network can generally be viewed as the network between the field RTU's and PLC's to the Control Firewall between the IT and OT networks. But in the real world, things are never that neat. Where does IT end and SCADA begin? How does the process of accessing this network fit onto this image? The truth is that this process is like art, the line has to be drawn somewhere.[33] Some companies might have the Control Firewall as the hard point between SCADA and IT, while other might have it at the Human Machine Interface (HMI) station. Chances are the boundaries are never firm. For example, if a controller is monitoring SCADA assets from the HMI station and there is a problem with the machine, will he call IT or SCADA for help? The answer is, it depends. If the issue can't be resolved from fixing something with a SCADA product, then it will be pushed to IT. However, if the problem is IT or the result of an IT security policy, like blocking "unused" ports, then chances are that SCADA will make the changes required to get the data from the field at the expense of IT's security policy.[34] This gets at the heart of the problem, which is the fact that SCADA is not an extension of IT, but a wholly separate entity.

SCADA prioritizes the availability of data while IT departments prioritize the confidentiality of data.[35] This is not to say that any one department is to blame for SCADA cyber vulnerabilities, but that by doing their jobs correctly, each department perpetuates the current dynamic. After all, it's the SCADA department that will get the angry email if flow and billing data is missing at the end of the month. This dynamic is the point where the realities of SCADA networks begin to create security problems. As was evident in the previous section, when hackers target SCADA they target the field equipment. With heavy procurement, installation, maintenance, and operational costs, field equipment is the most expensive and important equipment in an ICS company. Especially so once the cost of lost business and regulatory violations of equipment failure are taken into account. Field equipment is also the weakest point. Since many field sites are in geographically remote locations, it is logistically and financially difficult to maintain, update, and replace them. As a result of this reality, the equipment used in SCADA networks is designed to last as long as possible, which in some cases leaves equipment operating in the field for twenty or

thirty years. As new technology emerges that lets more data come into the office faster, SCADA departments find themselves with just enough time and resources to bring their legacy equipment up to the lowest point of compatibility with modern communications technology. This means that most field equipment is relying on technology that is decades older than the technology used by hackers to exploit them. On top of that, most of this equipment is designed to do a specific task as reliably, efficiently, and safely as possible. SCADA devices are not designed to be security devices. Chances are, the web browsers used in a company with a SCADA system have the capability to use the latest security technologies, like TLS 1.2, because they were designed to. This is not the case for SCADA devices. Trying to add a security component to a compressor and another one to a transmitter won't make either device more secure, it will just make the network harder to use.[36] Lastly, SCADA equipment is designed as a static form of defense against the elements. ICS companies have precise equations that let them know exactly how much flow a pipe of a certain diameter can handle at a certain temperature. These numbers will never change because they're based in physics. But cybersecurity is not static. The adversary is other people, not nature, so what works as a defense today, may be irrelevant in a year. However, this fact does not change many companies approach to defending SCADA networks.

There is a belief that safety logic will be able to prevent a cyber-attack, however faith in this is not well founded. Safety logic is designed to protect ICS against automation. If a pressure climbs too high either by accident or design, the safety logic will kick in and alleviate the pressure. However, safety logic might not be able to handle conditions that arise as a result of a series of purposeful and malicious changes to environment variables as was the case with the German steel mill attack. It is also safe to assume that if a hacker has the capability to penetrate deep enough into a system to manipulate valves, that the safety logic itself could be altered. Another tactic commonly misconstrued as an effective cybersecurity policy is air-gapping, or isolating your SCADA network entirely from the rest of the company's networks. While it does give a degree of security, it is only a stop-gap. At some point, data must get from the SCADA network to the IT network. If the data is transferred by USB stick or external hard drive, malware can still enter the SCADA network. It was through a USB stick that the malware Stuxnet managed to infect the isolated network of Iran's nuclear program. Even if there are a series of "controlled" entry points into the SCADA network, these can still be difficult to control in practice. As Sean McGurk, the former director of the National Cybersecurity and Communications Integrations Center at the DHS, stated during a congressional hearing, "…in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network. On average, we see 11 direct connections between those networks and in some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise environment."[37] What if one of those connections was used by a hacker to access a SCADA network? Even with isolated networks in place, there are still over 2 million ICS devices connected directly to the internet.[38] A number which includes 93,793 Modbus TCP/IP devices listening on port 502 open on the Internet.[39] Even if it's not considered part of "the Internet" by its users, SCADA is connected to more than just the next device along the network. Beyond network isolation and besides safety logic, what now stands between the most valuable assets of the company and hackers?

The last great difference between IT and SCADA that makes IT security policy fail when pushed out to the SCADA field, is how each one handles a hack. When IT gets hacked, the hackers are usually just after money.[40] The only damages are to the company's finances and reputation. IT can swiftly (when compared to SCADA) react. The affected hardware is likely nearby and likely has the latest software version installed. Affected equipment can be isolated to contain the attacks and replaced. Backups probably exist so that downtime will not be that extensive. SCADA networks are a bridge between the cyber world and the physical world. At some point, a click on a screen is translated into kinetic motion. Since that motion could be to cause damage to equipment, the damages from hacking a SCADA network could be measured in human life. Since the equipment is geographically isolated, it would be very difficult to repair or replace all the infected equipment. It's not even clear if there will still be equipment to repair. With these fundamental differences between IT and SCADA understood, the case for a distinct SCADA cybersecurity policy need not be made, it should only be observed and once observed, acted on.

Crafting SCADA Security: Policy as Process

The functional differences between IT and SCADA that created the context for hackers to succeed are the same differences that necessitate a separation of SCADA security policies from IT policies. This is not to say that the two are opposites or that there is not a functional working point between them. Rather, this is the assertion that security policies are only effective when they can be implemented, so if a policy is designed for one department but enforced in another it secures nothing. Imagine a cybersecurity policy like a pane of glass for a window. Its purpose is to protect you from the elements outside. Now if you have two different shaped windows, IT and

SCADA, you need a pane for each one. Sure, the window pane fits the IT frame, but when you try to force it into the SCADA frame it shatters. For example, the IT policy might require all machines to apply software patches within a certain timeframe of their availability.[41] Often, this process would require extensive testing on redundant SCADA machines and might not even be possible with the hardware or software that's run on some sites. IT also has the option of standardizing key components of communications technologies, like uniform firewalls and the same anti-virus program on each machine. SCADA often does not have control over what radios, satellites, or field equipment is used because of the way acquisitions and logistical realities often play out, increasing the complexity of the network and forcing more attention to be put on basic maintenance of the system. Crafting a viable cybersecurity policy for SCADA networks that makes it outside of a board room requires "entirely new approaches."[42] When viewed as a goal, this task seems impossible, but when understood as a process, it's wonderfully achievable.

Cybersecurity is not equivalent to cyber certainty. No cybersecurity professional uses the words "impossible" when describing the chances of an attack succeeding. Cybersecurity exists as a spectrum, not a binary state of safe or unsafe.[43] The safest SCADA system would be one where no one has access to it and the easiest to use would be a system with no security checks. Good cybersecurity policy is built by finding a balance between a company's business needs and security needs. Dreaming-up a bunch of what-if scenarios when creating cybersecurity policies shifts the focus of the discussion away from the applicable and becomes just another meeting. Only by focusing on the actionable, can policymakers achieve the doable. The examples of hacks provided earlier serve as a baseline for understanding what SCADA truly faces so that policy measures can be taken to minimize the risks to SCADA systems and maximize security. There is no better way to understanding risk than by quantifying it.

Determining what needs to be defended, is an exercise in risk mitigation. Once the risks are revealed and their costs understood, policies can move to reduce their potential negative impact on the business. The risks SCADA faces are environmental, regulatory non-compliance, financial, and most importantly, safety. SCADA hacking is estimated to have already killed as many as 1000 people.[44] If these risks can be boiled down to their component liabilities, then the urgency for an active SCADA policy becomes evident. The average cost of a successful hack attack without loss of human life or environmental damage is $7.01 million.[45] The Turkish pipeline explosion discussed earlier released over 30,000 barrels of oil into an aquifer and cost the operating company $460 million in lost business during the three months it took to fix the pipeline.[46] With such high costs, many companies turn to insurance to help reduce the company's exposure, but insurance companies themselves are also struggling with understanding today's cyber realities.

Imagine a large industrial facility that houses multiple companies' employees and assets that is targeted in a cyberattack that causes catastrophic damage to the facility. Workers, first responders, and nearby civilians are killed and injured in the explosion.[47] Will the company's cyber insurance cover this cost? This exact scenario is what the global insurer Lloyd's is preparing for. However, even they state that they are still "developing" their understanding of these kinds of attacks. Insurance companies do not have a standard by which to assess and then accurately insure SCADA assets. This is because each company has "unique risks" where "customized coverage" is required.[48] Even when coverage is obtained, exclusions will include bodily harm and property damage.[49] What this means is that insurers are more likely to use a company's cybersecurity policy and underwrite the risks based on compliance with them. More than likely, the companies that suffered the attack described at the beginning of this paragraph will not be covered. Insurance often has exclusions or add-ons in it for terrorism and state-sponsored attacks, which tripled last year.[50] But the line between cyber-war and cyber-terrorism is blurry.[51] Is it terrorism or a state-sponsored attack if Iran hacks a SCADA system? There is also the issue of compliance. If a company's insurance is based on adherence to the company's cyber policy then how well that policy is implemented becomes the key to a company's coverage. If a cybersecurity policy states that all field equipment will be reconfigured before deployment to the field so no default settings or default vulnerabilities are present an insurer would have cause to dispute compliance if any equipment is found to still have default settings on it after an attack. When dealing with SCADA networks, the chances of that are high. Because of the nature of these threats, SCADA departments must take it upon themselves to create their own policies.

Constructing a cybersecurity policy is not just the purview of IT departments, "it is an enterprise-wide opportunity."[52] Rather than just an opportunity for defense, cyber-security is viewed as an opportunity for growth. Adopting and maintain cyber-technologies gives companies a competitive advantage because it allows for new productive technologies to be integrated safely into a network instead of shunned.[53] Every department with a cyber presence needs a cybersecurity policy. Increasingly, CEO's of all industries see cyber risks as their top risk.[54] This is not likely to change anytime soon. Also unlikely in the near future are government regulations that will alleviate the need for SCADA departments to create their own policies.[55] The Executive branch did conclude that "it is undeniable that an appropriate level of cybersecurity cannot be achieved without regulation, as market forces

alone will never provide the level of security necessary to achieve national security objectives."[56] However, changing this "undeniable" truth into a policy proved impossible for the government as the regulations became bogged down in Congress when they tried to create a one size fits all policy.[57] This is not to say that the government can't be a part of a cybersecurity process, but SCADA departments can't wait for government regulations to dictate a security policy to them. A fundamental truth of security policies, especially when it comes to networks as geographically and technologically diverse as SCADA, is there is no standard security policy. National Security Agency director, General Mike Haden, hinted at this same idea when he said, "With no common knowledge, no meaningful discussion, and no consensus… the policy vacuum continues."[58] It is important that the cybersecurity policy created for SCADA network does not itself, operate in a vacuum. The SCADA security policy must work well with the IT policy since they are both there to defend the same entity. Again, we're trying to fit a pane of glass into a window frame, not make a new room around the window. A good place to use as a touchstone for new or improved security policies are existing guideline documents.

There are troves of documents that outline the approaches and considerations for cybersecurity policy creation.[59] They cover topics such as health risks, property risks, environmental risks, financial risks, reputational risks, and safety risks. To examine each of these would be beyond the scope of this paper, but an understanding of their role in the wider cyber policy creation process is required for the final recommendations to have context. One of the most prominent guidelines for cybersecurity policies is the *Framework for Improving Critical Infrastructure Cybersecurity* from The National Institute of Standards and Technology. This outlines 22 steps amongst five stages of creating and implementing a cybersecurity policy. It would be easy, and indeed likely recommended, to have made this the backbone of the paper, however, the goal of this paper is not to be one of the hundreds of interpretations of *Framework,* it is to give SCADA practitioners ideas to take to the test lab. Indeed, even if *Framework* was the focus, it would fail the goal of this paper. While *Framework* makes no specific technology recommendations; it's a very useful guideline, but not a cure-all.[60]

Industries have also been busy creating their own guidelines and standards. The International Society of Automation (ISA) created ISA-99 or ISA-62443, which is a comprehensive application of cyber security practices broken into 13 documents. For example, in ISA-62443-4-1 the strategy known as defense in depth is endorsed and explained in a manner that can be taken directly to a board room.[61] However, papers 1-4, about use-cases for the standards, and 2-2, implementation guidance, are only in the planning phase.[62] While ISA99 will no doubt one day read almost like an instruction manual, it is not there yet. All these different standards want to do the same thing: move companies forward on cybersecurity. However, even when moving forward one can still be traveling in a circle. Therefore, a course must now be set that plugs the gap between IT and SCADA, prevents as many attacks as probable, mitigates as much risk as possible, and works within the realities of what SCADA networks need.

SCADA Security: Process Protector & Business Enabler

The first step in creating effective policy is identifying the company's strategically important assets.[63] For SCADA networks, the most important and most vulnerable assets are the field assets. It's evident from the examples discussed earlier that when hackers target ICS systems they ultimately want to obtain access to field equipment. Due to the geographic and environmental factors of field equipment, pushing IT's security solutions out to the field often fails. The financial and moral costs of not protecting the most volatile assets of a company also presses this point home. Because of the destructive and sensitive nature of field equipment's safety, it's imperative for SCADA's cybersecurity policy to focus on preventing hackers from having access to this equipment.[64] After all, once malware runs on an endpoint machine, it's too late.[65] The equipment can then be programmed or commanded to cause destruction. It's true that mitigation strategies are also important, but the focus of this paper is on the initial, preventative layer of protection since that is the first barrier to an attack and the one most actionable by SCADA stakeholders. Prevention is about asserting control over a network by controlling who has access to the data and equipment on a network. SCADA can assert control even when its priority is data availability through technologies with security designed into them.

The next step in creating a viable cybersecurity policy is selecting technologies to defend the priority assets. Effective cyber security policies protect a company without disrupting business. This means looking for opportunities to design security into a process rather than bolting-on a feature. Bolt-on technology is a consequence of not applying the most efficient solution from the beginning, thus forcing future projects to pay this debt.[66] SCADA's problem is that "many of the critical components that operate today do so in a context that's completely different from the one they have been designed for."[67] Cybersecurity wasn't as dangerous a threat to networks whose foundations were laid even ten years ago. This often forces SCADA departments to use adaptive technologies as stand-alone solutions for individual devices, like having to add a terminal server to a site. This

reality is comparable to gluing a window shut instead of installing a window lock. Sure, the window is closed, but now it's just a glass wall. If the context changes so the window needs to open what then? Perhaps the window was glued because locks weren't in the budget or the employees weren't trained in locks. The reasoning for bolt-on is easy to defend, the networks they create are not. For example, a company decides to use passwords on its field equipment, so it creates a password for its transmitters, compressors, and RTU's. Rather than provide security, it makes the network harder to use on a day-to-day basis. The real-world result of this solution is that the password will be left as a default to allow everyone access. The network is not more secure it's just slightly harder to use.

Designing security into a process is about changing the insecure procedure's structure. Security isn't operating on top of a network, but as part of the network. To keep up with the analogy, it's buying the windows with the locks already on them. For example, installing a device at the field level that could secure communications between each field site and the SCADA office refashions the process of accessing the equipment and transmitting the data. Taking the legacy equipment issues of SCADA systems into account, the difference between the examples just discussed can be hard to see. The nuance is not so much in how a solution is physically applied, but about how it affects the process. If a solution addresses the problems a network has today, it can be bolt-on or designed-in. If it can grow with a business and change in response to future threats, it's designed in. One of the best technologies for securing today's and tomorrow's networks is encryption.

Encryption is the process of using complex mathematical equations to encode a message in so that only authorized entities can decrypt and then read the message. Basically, a very large number is entered into an equation that scrambles messages and the only way to make the messages readable is to know the right number to use for the decryption equation.[68] Currently, "encryption is much less common in low-level applications, such as communications between control system software and PLC's and RTU's."[69] SCADA already deals with a different protocol for every vendor's hardware, but encryption is owned by no one entity so users won't be locked into one encryption vendor. In fact, vendors that sell proprietary encryption methods should be avoided as this is another form of security through obscurity. There are open standards for encryption which are based on "sound mathematics" for their defense.[70] These open standards of encryption generally come in two forms, symmetric AES and asymmetric RSA. Now, the technical mechanics behind these encryption methods is not important for the purposes of this paper. These are standard methods with libraries of information available. What's important for this paper is discussing how to deploy them and how they benefit SCADA networks.

AES encryption allows both ends of a network to encrypt and decrypt messages by distributing a "secret-key" to each part. The problem with this is that each end must have the same key and anybody with a copy of the one secret-key can join the network. RSA uses a private decryption and a public encryption key. The private key is kept secret by the receiver, but the public key is open for anyone to use. Messages sent to the receiver using the receiver's public key can only be read by the entity with the corresponding private key. So if both ends of a network have their own private key and the other end's public key, they can communicate securely. The trouble with this method is that it is computationally demanding, meaning that in the context of SCADA it could create network lag if used excessively. AES and RSA encryption can be used separately or together. Generally, when they're used together they're used in the form of a public key infrastructure (PKI.) This allows the strength of one counter the weakness of the other.

A PKI is a way to automatically create and control a rotating series of symmetric keys between communicating entities as a way of controlling which machines, programs, and people have access to a network. PKI's use algorithms to create certificates with unique pairs of public and private keys. These asymmetric keys are then used to share the symmetric key. These certificates can be password protected which requires network users to have knowledge of the password and possession of the certificates for network accessibility. This combines both symmetric and asymmetric encryption technologies into one system. Here, the vulnerability symmetric keys have of allowing anybody with the right secret-key to access the network is negated, since a PKI can automatically generate and distribute new symmetric keys every session. These new keys are exchanged using asymmetric encryption at the beginning of a connection. Since symmetric keys have much lower overhead on a network than asymmetric keys do, using asymmetric encryption once in order to then use symmetric encryption prevents PKI technologies from creating heavy network lags.[71] This makes encryption technology through PKI deployment ideal for SCADA networks.

Encryption provides the ability to create data integrity through integration, data availability through confidentiality, and ultimately, safety through security. It is also usually a requirement for any network trying to obtain cyber insurance.[72] Data coming from the field or commands sent from the office only has value if it's correct. PKI's give data confidentiality by preventing any unauthorized user from reading the data. Since all the data is encrypted, an intercepted message would be meaningless to a hacker. This is important because it prevents

attackers from mapping out a network by reading the traffic. Now if a hacker had a zero-day exploit or one of the 400 known SCADA hardware vulnerabilities, but did not know the location of the equipment for that exploit then this attack is negated.[73] It should be mentioned, that encryption should not interfere with field devices native protocols. Encryption is added to a message when it is on the IP layers of a communication channel, so it is compatible with the equipment that already exists in the field. However, it does help shield SCADA device protocols from being exploited.[74] PKI's also provide SCADA networks with integrity by protecting data from modification. This prevents hackers from intercepting a message, making alterations to it, and sending it back out to the network. If any part of an encrypted message is changed then the decryption process will fail and the message will be discarded. An encrypted message cannot be recorded and played back, since the encryption of each message has a timeout associated with it. One implication of this is that the encryption device, the device doing the encryption and decryption, acts as a gateway, preventing non-encryption or corrupted messages from passing through to the devices behind it. This fundamental mechanic of encryption makes it ideal for deployment in SCADA networks.

As this paper has established the field equipment as the most vulnerable and dangerous part of a SCADA network, a strong SCADA cybersecurity solution must be focused on directly protecting field equipment. For example, if a farmer was having trouble with rabbits stealing his crops he'd put a fence around his garden, not his house. In the same spirit, SCADA departments should deploy encryption devices at the field level. Attempts to secure SCADA networks in this manner have failed up to now largely because SCADA's geographic diversity undermined the proximity required for successful IT security solutions. However, in this context, SCADA's geography is actually a cybersecurity strength. Since each field site is in some way remote and has multiple devices per site, it's impossible to have every single field device connect directly to the control system. Usually, field devices connect to one device (RTU or PLC) that then sends the data to the control room. This creates a choke-point for network communications, which allows a defense to occupy that point and limit the attack surface of a network, thus reducing the chances of a successful attack. Therefore, SCADA networks should deploy encryption devices strategically at the RTU or PLC level to secure a network's traffic and equipment. The strategy of a "device level" solution is also recommended by organizations such as Symantec, Dell, and the United States Government (USG).[75] This solution allows for the latest cybersecurity technologies to defend what cannot defend itself. This point is further strengthened by the physical and computational limitations of existing field equipment. It's currently impossible for existing field equipment to be configured to use encryption. A transmitter or valve simply doesn't have the hardware to run encryption technologies. Just as radios and satellites were integrated into SCADA systems, so too must encryption devices be integrated into the field.

Although financial and logistical arguments will be made against such a proposal, these are current-quarter issues that revolve around localized office politics. The magnitude of SCADA vulnerabilities necessitates a discussion that creates results. Without it, cybersecurity solutions will be added as afterthoughts and in piecemeal if at all. It should be noted, that the successful SCADA protocol DNP3 has security capabilities, but this does not make it the solution SCADA networks need. First, DNP3 was not "designed with security in mind."[76] The security features of DNP3, versions 2 and version 5, were additions to the protocol in response to client needs. While the protocol continues to function wonderfully for its designed purpose, the security successes have been mixed. DNP3 is specifically labeled as "not encryption" by the Distributed Network Protocol organization itself.[77] It's presented as an enhancement in end-to-end security. While this is true within a specific context, relying solely on a device protocol to secure a whole network breaks down in the field. Second, DNP3 is implemented by individual vendors without a regulatory compliance structure because it was designed to be an open and available standard. Having DNP3 from one vendor is not the same as having DNP3 from another vendor. As a testament to this point, ICS-CERT recently released a report that 18 vendors of DNP3 had serious security flaws with their implementation of DNP3.[78] Lastly, DNP3 is not itself a cybersecurity policy solution for an industrial internet of things network. Part of ICS-CERT's recommendation on how to properly deal with the vulnerabilities mentioned earlier was to "ensure that [DNP3 devices] are not accessible from the Internet." [79] The purpose of these points is not to single out DNP3 (since it is industry foundation) but to further highlight the need for the inclusion of a device at the field level that anchors a cybersecurity policy. Without knowing the nuances and subtleties of a SCADA network, a recommendation for a specific device would be at best misguided and at worst a sales pitch. Therefore, the conclusion this paper arrives at for securing SCADA networks by utilizing encryption technology that's designed into the wider network as part of an integrated SCADA cybersecurity policy is to use FIPS 140-2 devices.

The Federal Information Processing Standards (FIPS) 140-2 is a series of security requirements for applying cryptography to the field. FIPS 140-2 was created through a collaboration of the National Institute of Standards and Technology of the US and the Communications Security Establishment of Canada as a best-practices guide for implementing specific cybersecurity technologies. Questions like "What type of encryption should I use?" and "What are the best practices for password and certificate management?" are answered when a FIPS device is used.

FIPS has requirements for implementing PKI's and both AES and RSA encryption. If a company wants to be a supplier of communications technology to the USG for critical, but not classified, communications then the technology must be certified as a FIPS 140-2 compliant.[80] For an example of a critical communication, the communication between US navy ships at sea is done through FIPS certified technologies.[81] FIPS 140-2 is a voluntary form of regulation. If a company wants access to the government's checkbook, it will adhere to these standards. Although this paper's recommendation is for a FIPS 140-2 device, hardware, software, and firmware can each and all be certified as FIPS 140-2 compliant.[82] FIPS 140-2 has four levels of compliance allowing for FIPS 140-2 software to sit on a server while a FIPS 140-2 level 2 device anchors the technology out in the field.

Critics of FIPS 140-2 point to the fact that the process of becoming FIPS 140-2 certified takes roughly 4 to 12 months and costs tens of thousands of dollars. This then limits the updates that can be made to a device and limits development on the devices since software development cycles are shorter than FIPS validation cycles.[83] Let's allow for context to pose a counterpoint. For ICS industries, hardware lifetimes are often decades and travel time between field sites can be measured in months on a timesheet, so the idea of FIPS 140-2 falling behind software development is moot. ICS company's need devices that are produced for security and are proven to provide security so that the costs can be justified and the risks mitigated. FIPS 140-2 can provide such devices precisely because there is a validation process. Well-developed cybersecurity standards like FIPS 140-2 enables consistency among product developers and serves as a reliable metric for purchasing security products since a validation certificate proves that cryptographic technologies have been correctly implemented by an impartial third party.[84] In an industry like cybersecurity, where there is still uncertainty if cybersecurity is two words or one[85], FIPS 140-2 provides the kind of guidance that helps technology improve security by leaps instead of moving forward towards cyber goals inch-by-inch. In point of fact, the market realities around the FIPS 140-2 validation process actually helps maintain security for field devices.

A FIPS validation only lasts five years, at which point it must again go through the validation process.[86] This cycle alone would mean that a FIPS device would get more development attention than most equipment already deployed in SCADA networks. It's also important to note that FIPS 140-2 changes its validation requirements in response to changing cyber-environments. A FIPS device validated two years ago underwent a slightly different testing than one that does the validation this year. Another benefit of the validation process is how it incentivizes vendors to make updates to their own products in response to evolving cyber threats. Since a FIPS 140-2 validated certificate is required for doing business with the USG, companies are voluntarily complying with FIPS to maintain access to that market. There are thousands of FIPS devices that can act as terminal servers, routers, firewalls, or whatever type of device a SCADA field might need. These devices come from big name companies too as can be seen by a quick glance at the NIST's list of validated modules.[87] This market force keeps FIPS devices up-to-date since the government would not tolerate waiting 6 months or a year to implement security. If a vulnerability does develop then FIPS devices can receive updated software, if the creators included the ability to update software. There is nothing that stops new software from being deployed on a FIPS device, however doing so could invalidate its legal claim to being FIPS. When the Heartbleed Bug came out in 2014 it forced the FIPS 140-2 certified software library OpenSSL to react swiftly.[88] For SCADA, this should be welcomed news. For example, Stuxnet infected a pressure transmitter that is common in the oil and gas industries, but the vendor denied it had been hacked for 6 months after the vulnerability was detected.[89] It then took another two years for a fix to be released. Considering the geographic diversity of these transmitters in the field, how much longer would it have taken to implement the fix? Going through the validation process and maintaining relations with the USG also shows a company's commitment to the product. This should comfort SCADA network managers since they would be less likely to be found choosing a FIPS device, only to have it discontinued. FIPS 140-2 also lays the foundation for government regulations. If the USG managed to create regulations for all ICS industries in response to a major event, chances are those regulations will use existing voluntary regulations as a starting point. Using this logic, FIPS is a way to not only identify which products actually implement cryptography well, but help identify which devices have a long life.

The usefulness of FIPS 140-2 to any industry can be seen from how cyber insurers use it. FIPS 140-2 is listed as a recommended industry standard for developing an insurable cybersecurity policy. One of the features that endears insurers to FIPS is that FIPS displayed when it is and is not in FIPS mode. On some devices FIPS mode can only be triggered if the default password and PKI configurations are changed from their out-of-the-box defaults. This helps ensure both compliance to a cyber insurance plan and compliance to FIPS. FIPS also requires validated devices to have a security policy outlining exactly how to configure a device to be in FIPS mode. One of the benefits of having a documented process like this is that it allows for the device, and therefore the cybersecurity policy it embodies, to be implemented. Cybersecurity efforts begin with people, which is also where many cyber incidents also begin.[90] Therefore, the most important aspect of a cybersecurity policy is how easily it is implemented properly. When a process is documented it is formalized. When it's formalized it's consistent and

when it's consistent people understand what they need to do. Unlike some standard pieces of SCADA equipment, a FIPS device cannot be deployed in FIPS mode with default settings. This overcomes one of the greatest hurdles to implementing any cybersecurity policy. To make this discussion more industry relevant, FIPS 140-2 is also endorsed either directly or in parallel agreement with several ICS industry produced guidelines. The ISA recommends FIPS 140-2 when "protecting highly valuable control system data and information" because "only units that can be certified to comply with a standard, such as FIPS 140-2," can "ensure that cryptographic systems were studied carefully for weaknesses by a wide range of experts, rather than being developed by a few engineers in a single company."[91] Ultimately, FIPS 140-2 is a way for SCADA departments to create state-of-the-practice realities out of state-of-the-art technologies.

Conclusion

SCADA and IT departments have created amazing networks that bring data in from the meanest field location with speed and reliability. But yesterday's connectivity is today's cyber vulnerability. With attacks against SCADA systems increasing in their frequency and potency every year, SCADA departments must create their own cybersecurity policies that address these threats without disrupting business. When viewed as an ongoing process rather than a one-time event, cybersecurity can be integrated into SCADA networks by focusing protection on the field assets with encryption since these are the most vulnerable and destructive parts of a SCADA network. The most effective and efficient method of achieving this is to deploy FIP 140-2 level encryption devices in front of the field assets themselves. These recommendations are by no means the only path to security, but they are the ones most ready for deployment and the most primed for returns. Therefore, the commendations made in this paper must be considered for SCADA network security in order to protect what's in the field now, allow for technological growth in the future, and put "control" back into SCADA.

Appendix A: Acronyms

This section describes the acronyms used throughout the document.

Acronym	Definition
AES	Advanced Encryption Standard
CA	Certificate Authority
CRL	Certificate Revocation List
CMVP	Cryptographic Module Validation Program
FIPS	Federal Information Processing Standard
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
RSA	Rivest Shamir and Adleman method for asymmetric encryption
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VPN	Virtual Private Network

Bibliography

[1] "Huge jump in ICS Attacks." Industrial Safety and Security Source. December 29, 2016. Accessed January 1, 2017. http://www.isssource.com/huge-jump-in-ics-attacks/.
[2] Small, Prescott E. Defense in Depth: An Impractical Strategy for a Cyber World. Publication. SANS Institute. 2012. Accessed January 5, 2017. https://www.sans.org/reading-room/whitepapers/assurance/defense-depth-impractical-strategy-cyber-world-33896, p.12
[3] Shawn Henry, "Top 5 Cybersecurity Mistakes Companies Make and How to Avoid Them," *CrowdStrike Blog*, January 6, 2017, https://www.crowdstrike.com/blog/category/endpoint-protection/.
[4] Dave McMillen, "Attacks Targeting Industrial Control Systems (ICS) Up 110 Percent," *Security Intelligence*, December 27, 2016, accessed January 6, 2017, https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/.
[5] *2015 Dell Security Annual Threat Report*, Dell, 2015, https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf, p. 12
[6] "U.S. Has Most Internet Connected Industrial Control Systems," *SecurityWeek*, July 11, 2016, accessed January 5, 2017, http://www.securityweek.com/us-has-most-internet-connected-industrial-control-systems.
[7] Nicole Perlroth, Elizabeth A. Harris, "Cyberattack Insurance a Challenge for Business," *The New York Times*, June 8, 2014, accessed Jan 5, 2017, https://www.nytimes.com/2014/06/09/business/cyberattack-insurance-a-challenge-for-business.html.
[8] "Dell Annual Threat Report analyzes the most common attacks observed in 2014 and how emergent threats will affect organizations throughout 2015," *Dell*, March 13, 2015, accessed January 4, 2017, https://www.dell.com/learn/us/en/vn/press-releases/2015-04-13-dell-annual-threat-report.
[9] "NCCIC/ICS-CERT Year in Review," *Industrial Control Systems- Center of Cyber Emergency Response Team*, 2016, accessed November 2016, https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf, p. 6. Note: at the time this paper was written, the Year in Review report for 2016 was not yet available.
[10] Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar," *Bloomberg*, December 10, 2014, accessed March 15, 2016, https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.
[11] Robertson and Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar," , https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.
[12] Kyle Wilhoit, "Who's Really Attacking Your ICS Equipment?" *Trend Micro*, 2013, https://media.blackhat.com/eu-13/briefings/Wilhoit/bh-eu-13-whose-really-attacking-wilhoit-wp.pdf, p.10
[13] Kyle Wilhoit, "The SCADA That Didn't Cry Wolf," *Trend Micro*, 2013, https://media.blackhat.com/eu-13/briefings/Wilhoit/bh-eu-13-whose-really-attacking-wilhoit-wp.pdf, p.22
[14] Time Simonite, "Chinese Hacking Team Caught Taking Over Decoy Water Plant," *MIT Technology Review,* August 2, 2013, https://www.technologyreview.com/s/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/.

[15] "The Dark Side of the Cloud," Techopedia, December 9, 2016, https://www.techopedia.com/2/28119/trends/cloud-computing/the-dark-side-of-the-cloud.
[16] Jordan Robertson, "How Private Data Became Public on Amazon's Cloud," *Bloomberg*, March 27, 2013, https://www.bloomberg.com/news/2013-03-26/how-private-data-became-public-on-amazon-s-cloud.html.
[17] Kyle Wilhoit, "SCADA in The Cloud," *Trend Micro*, 2013, https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-scada-in-the-cloud.pdf, p. 5
[18] Wilhoit, "SCADA in The Cloud," , https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-scada-in-the-cloud.pdf, p. 6
[19] Kim Zetter, "A Cyberattack has Caused Confirmed Physical Damage For the Second Time Ever," *Wired*, January 8, 2015, https://www.wired.com/2015/01/german-steel-mill-hack-destruction/.
[20] Zetter, "A Cyberattack has Caused Confirmed Physical Damage For the Second Time Ever," https://www.wired.com/2015/01/german-steel-mill-hack-destruction/.
[21] Edward J. M. Colbert and Alexander Knott, "Cyber-security of SCADA and Other Industrial Control Systems," (Springer, 2016), p. 128. The exact note "For ICS, the relevant actor in the Cyber Attack taxonomy is typically state-sponsored." I paraphrased the spirit of the chapter.
[22] President Barack Obama, "Statement By The President On First Step Agreement On Iran's Nuclear Program," November 23, 2013, https://www.whitehouse.gov/the-press-office/2013/11/23/statement-president-first-step-agreement-irans-nuclear-program.
[23] "Cyber Threats to the Nordic Region," *FireEye*, May 2015, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-nordic-threat-landscape.pdf, p. 16
[24] "Cyber Threats to the Nordic Region," *FireEye*, p. 14
[25] "2015 Dell Annual Security Threat Report," *Dell*, 2015, https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf, p. 8
[26] Laura Smith-Spark, "Why is Russia sending bombers close to U.S. Airspace?" *CNN*, July 27, 2015, http://www.cnn.com/2015/07/27/world/us-russia-bombers-intentions/.
[27] "Operation Cleaver," April, 2015, https://www.cylance.com/operation-cleaver-cylance
[28] Garance Burke and Jonathan Fahey, "investigation: US Power Grid Vulnerable to Foreign Attack," *PHYS.ORG,* December 21, 2015, http://phys.org/news/2015-12-power-grid-vulnerable-foreign-hacks.html
[29] James Andrew Lewis, "The Rationale for Offensive Cyber Capabilities," June 8, 2016, https://www.csis.org/blogs/csis-strategic-technologies-blog/rationale-offensive-cyber-capabilities
[30] Lewis, The Rationale for Offensive Cyber Capabilities."
[31] "No Such Thing as Hacker-Proof," *Deloitte,* December, 2013, http://deloitte.wsj.com/cio/files/2013/12/The-Next-Big-Idea-in-Cyber-Security-INFOGRAPHIC-revise.pdf, p. 1
[32] "SCADA," *Wikileaks*, https://en.wikipedia.org/wiki/SCADA
[33] Gilbert Keith, "Art, Like Morality, Consists of Drawing the Line Somewhere," *Quote Investigator*, http://quoteinvestigator.com/2014/07/20/drawing/
[34] [34] Eric Forner & Brian Meixell, "Out of Control: Demonstrating SCADA device exploitation" (presentation and demonstration presented at the Black Hat USA 2013 convention, Las Vegas, Nevada, December 3, 2013) https://www.youtube.com/watch?v=FTzAkEnwx_c
[35] ISA99, Industrial Automation and Control Systems Security Committee, "NIST Cybersecurity Framework: ISA99 Response to Request for Information," April 5, 2013, http://csrc.nist.gov/cyberframework/rfi_comments/040513_international_society_automation.pdf, p. 3
[36] ISA99, "NIST Cybersecurity Framework: ISA99 Response to Request for Information," http://csrc.nist.gov/cyberframework/rfi_comments/040513_international_society_automation.pdf, p. 2
[37] *Cybersecurity: Assessing the immediate threat to the United States: Hearing before the subcommittee on National Security, Homeland Defense, and Foreign Operations of the Committee on Oversight and Government Reform, House of Representatives*, 112th Congress, 52, (2011) (Statement of Sean McGurk, the director of the National Cybersecurity and Communications Integrations Center at the Department of Homeland Security.) https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg70676/pdf/CHRG-112hhrg70676.pdf
[38] Joe Weiss, "Cyber Security of Industrial Control Systems (ICSs)," *Applied Control Solutions, LLC*, February 23, 2016, http://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_171119.pdf, slide 12.
[39] Tim Simonite, "Hacking Industrial Systems Turns out to Be Easy," *MIT Technology Review,* August 1, 2013. https://www.technologyreview.com/s/517731/hacking-industrial-systems-turns-out-to-be-easy/
[40] Yulia Cherdantseva , Pete Burnap , Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, and Kristan Stoddart, "A Review of Cyber Security Risk Assessment Methods for SCADA Systems," *Computers & Security* 56 (2016): 1-27.
[41] "Secure your Business Computers," *America's Small Business Development Center Los Angeles*, http://smallbizla.org/10-tips/secure-your-business-computers/
[42] ISA99, "NIST Cybersecurity Framework: ISA99 Response to Request for Information," p. 2
[43] Amadeo Pellicce, "Why Cybersecurity is a Spectrum, not a State," *Medium*, September 30, 2016, https://medium.com/warden-co/why-cybersecurity-is-a-spectrum-not-a-state-31bd7b1aea7e#.prwkahu8g.
[44] Weiss, "Cyber Security of Industrial Control Systems (ICSs)," http://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_171119.pdf, slide 19.
[45] "2016 Cost of Data Breach Study: United States," *Ponemon Institute*, June 2016, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094USEN, p. 6
[46] Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar," December 10, 2014, https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar/.
[47] "Lloyd's Cyberattack Strategy," *Lloyd's*, June 2016, https://www.lloyds.com/~/media/files/the%20market/operating%20at%20lloyds/lloyds%20cyber%20attack.pdf, p. 5. This exact scenarios is taken from their scenario outlining their own strategy.
[48] Judy Greenwald, "Cyber policies start to show their limitations," *Business Insurance*, July 17, 2016, http://www.businessinsurance.com/article/20160717/NEWS06/160719822/cyber-policies-start-to-show-their-limitations.
[49] Greenwald, "Cyber policies start to show their limitations," http://www.businessinsurance.com/article/20160717/NEWS06/160719822/cyber-policies-start-to-show-their-limitations.
[50] Perlroth and Harris, "Cyberattack Insurance a Challenge for Business," https://www.nytimes.com/2014/06/09/business/cyberattack-insurance-a-challenge-for-business.html.

[51] "Are Cyber War & Cyber Terrorism Insurable?" *Hodgson Russ Attorneys, LLP*, February 10, 2015, http://www.hodgsonruss.com/newsroom-publications-7855.html .
[52] Greg Bell, "Good Cybersecurity Doesn't Try to Prevent Every Attack," *Harvard Business Review*, October 25, 2016, https://hbr.org/2016/10/good-cybersecurity-doesnt-try-to-prevent-every-attack.
[53] Steve Martino, "How Cybersecurity is Enabling – Not Defeating – Business Innovation" *Cisco Blog*, July 20, 2016, https://blogs.cisco.com/security/how-cybersecurity-is-enabling-not-defeating-business-innovation
[54] "CEO's Mobilize for the fourth industrial revolution," *US CEO Outlook 2016 KPMG*, 2016, https://assets.kpmg.com/content/dam/kpmg/pdf/2016/07/2016-ceo-survey.pdf, p. 3
[55] The author is aware that some regulatory bodies already have regulations, like NERC CIP, however the understood audience for this paper is the oil and gas industry.
[56] Jerry Brito and Tate Watkins, "Loving the Cyber Comb? The Dangers of Threat Inflation in Cybersecurity Policy," *Harvard*, January 2012, http://harvardnsj.org/wp-content/uploads/2012/01/Vol-3-Brito-and-Watkins.pdf, p. 49
[57] Steve Bucci, Paul Rosenzweig, and David Inserra, "A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace," *Heritage Foundation*, April 1, 2013, http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace.
[58] Brito and Watkins, "Loving the Cyber Bomb?" http://harvardnsj.org/wp-content/uploads/2012/01/Vol-3-Brito-and-Watkins.pdf p. 80
[59] A notable one with transferable point to ICS is the NRECA's "Guide to Developing a Cyber Security and Risk Mitigation Plan, https://www.smartgrid.gov/files/CyberSecurityGuideforanElectricCooperativeV11-21.pdf. NIST also has a "Framework for Improving Critical Infrastructure Cybersecurity," https://www.nist.gov/sites/default/files/documents/2017/01/10/draft-cybersecurity-framework-v1.1.pdf
[60] Antony P. Kim, Aravind Swaminathan, and Emily Tabatabai, "FTC Makes Clear that NIST Cyber Framework is Not a Cure-All," September 12, 2016, http://blogs.orrick.com/trustanchor/2016/09/12/ftc-makes-clear-that-nist-cyber-framework-is-not-a-cure-all/.
[61] ISA99, "ISA-62443-4-1: Security for industrial automation and control systems," *ISA*, Draft 3, Edit 11, March 2016, p. 23
[62] ISA99 Committee, "ISA99: Developing the ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security," http://isa99.isa.org/ISA99%20Wiki/Home.aspx.
[63] Bell, "Good Cybersecurity Doesn't Try to Prevent Every Attack," https://hbr.org/2016/10/good-cybersecurity-doesnt-try-to-prevent-every-attack.
[64] "Operation Cleaver," *Cylance,* December 2, 2014. https://cdn2.hubspot.net/hubfs/270968/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf, p. 66
[65] *Cylance*, https://www.cylance.com/products-protect-critical-infrastructure
[66] Mario Chiock, "What is Technical Debt," Blog Post, November 7, 2016, https://www.linkedin.com/pulse/what-technical-debt-mario-chiock-cissp-cism-cisa-ciso?articleId=7429982034707257087#comments-7429982034707257087&trk=sushi_topic_posts
[67] Tiffani A Shields, "Prevention and Preparedness for Cyber Security Attacks and Incidents Against ICS/SCADA," *Saint leo University*, 2014, http://www.saintleo.edu/media/971751/prevention_and_prepardeness_for_cyber_security_attacks_and_incidents_against_ics-scada.pdf, p. 3
[68] A sample of an encryption key may be found at the following citation. The number was too large to print. "RSA Numbers," *Wikipedia*, https://en.wikipedia.org/wiki/RSA_numbers#RSA-768

[69] ISA-TR62443 – 3 – 1 Security for industrial automation and control systems, Security Technologies for Industrial Automation and Control Systems, Revision 2, p. 21
[70] "Guide to Cryptography," *The Open Web Application Security Project*, January 12, 2017, https://www.owasp.org/index.php/Guide_to_Cryptography
[71] Abdullah Al Hasib and Abul Ahsan Md. Mahmudul Haque, " A Comparative study of the Performance and Security Issues of AES and RSA Cryptography," *Helsinki University and Multimedia Laboratory*, 2008, https://www.researchgate.net/publication/232615754_A_Comparative_Study_of_the_Performance_and_Security_Issues_of_AES_and_RSA_Cryptography, p. 509
[72] "2016 Cyber Insurance Buying Guide," *Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security*, 2016, http://www.aba.com/Tools/Function/Documents/2016Cyber-Insurance-Buying-Guide_FINAL.pdf, p. 17
[73] Eduard Kovacs, "Over 400 Vulnerabilities Reported to ICS Cert in 2015," *SecurityWeek,* October 3, 2015, http://www.securityweek.com/over-400-vulnerabilities-reported-ics-cert-2015
[74] "Common Cybersecurity Vulnerabilities in Industrial Control Systems," *Department of Homeland Security, Control Systems Security Program*, May 2011, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf, p. 22
[75] Brian Meixell and Eric Forner ,"Out of Control: Demonstrating SCADA Device Exploitation," https://www.youtube.com/watch?v=FTzAkEnwx_c, 30:31
[76] "Keeping SCADA Networks Open and Secure," *Multitirode*, June 2008, http://www.multitrode.com/assets/assets/keeping-scada-networks-open-and-secure.pdf, p. 2
[77] "Why IEEE 1815 (DNP3) Secure Authentication?" https://www.dnp.org/DNP3Downloads/DNP3%20Secure%20Authentication%20Talking%20Points.pdf, p. 1
[78] "Advisory (ICSA-13-291-01B) DNP3 Implementation Vulnerability (Update B)," April 09, 2014, https://ics-cert.us-cert.gov/advisories/ICSA-13-291-01B
[79] "Advisory (ICSA-13-291-01B) DNP3 Implementation Vulnerability (Update B)," https://ics-cert.us-cert.gov/advisories/ICSA-13-291-01B
[80] "Security Requirements for Cryptographic Modules," *Federal Information Processing Standards*, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf, p. 55
[81] Cmdr. John MacMichael, "Navy Wireless Networks – FIPS 140-2 or Bust!" *CHIPS: The Department of the Nay's Information Technology Magazine*, July 2005, http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=3202
[82] "Security Requirements for Cryptographic Modules," p. iv
[83] Bruce Schneier, "OpenSSL Now FIPS 140-2 Certified," *Schneier on Security*, February 21, 2007, https://www.schneier.com/blog/archives/2007/02/openssl_now_fip.html
[84] Karen Scarfone, Dan Benigni, and Tim Grance, "Cyber Security Standards," *National Institute of Standards and Technology,* http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=152153, p. 1

[85] Joe Franscella, "Cybersecurity vs. Cyber Security: When and How to Use the Term," *Infosec island*, July 17, 2013, http://www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html
[86] "FIPS 140-2: Start selling into these markets," *Corsec*, https://www.corsec.com/certifications/fips-140-2/
[87] http://csrc.nist.gov/groups/STM/cmvp/validation.html, This link takes you to the validated module list.
[88] This link takes you to the FIPS 140-2 level 1 validation proof of security. Please note the validation dates. http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1747
[89] [89]Ralph Langner, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," *Langner,* November 2013, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf, p. 22
[90] Robert M. Lee, Michael J. Assante, and Tim Conway, "German Steel Mill Cyber Attack," *SANS Industrial Control Systems*, Dec 30, 2014, https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf, p. 12.
[91] "Technical Report Security Technologies for industrial Automaton and Control Systems," *ISA,* Revision 2, ISA-TR99.00.01-2007, 2007, p. 53