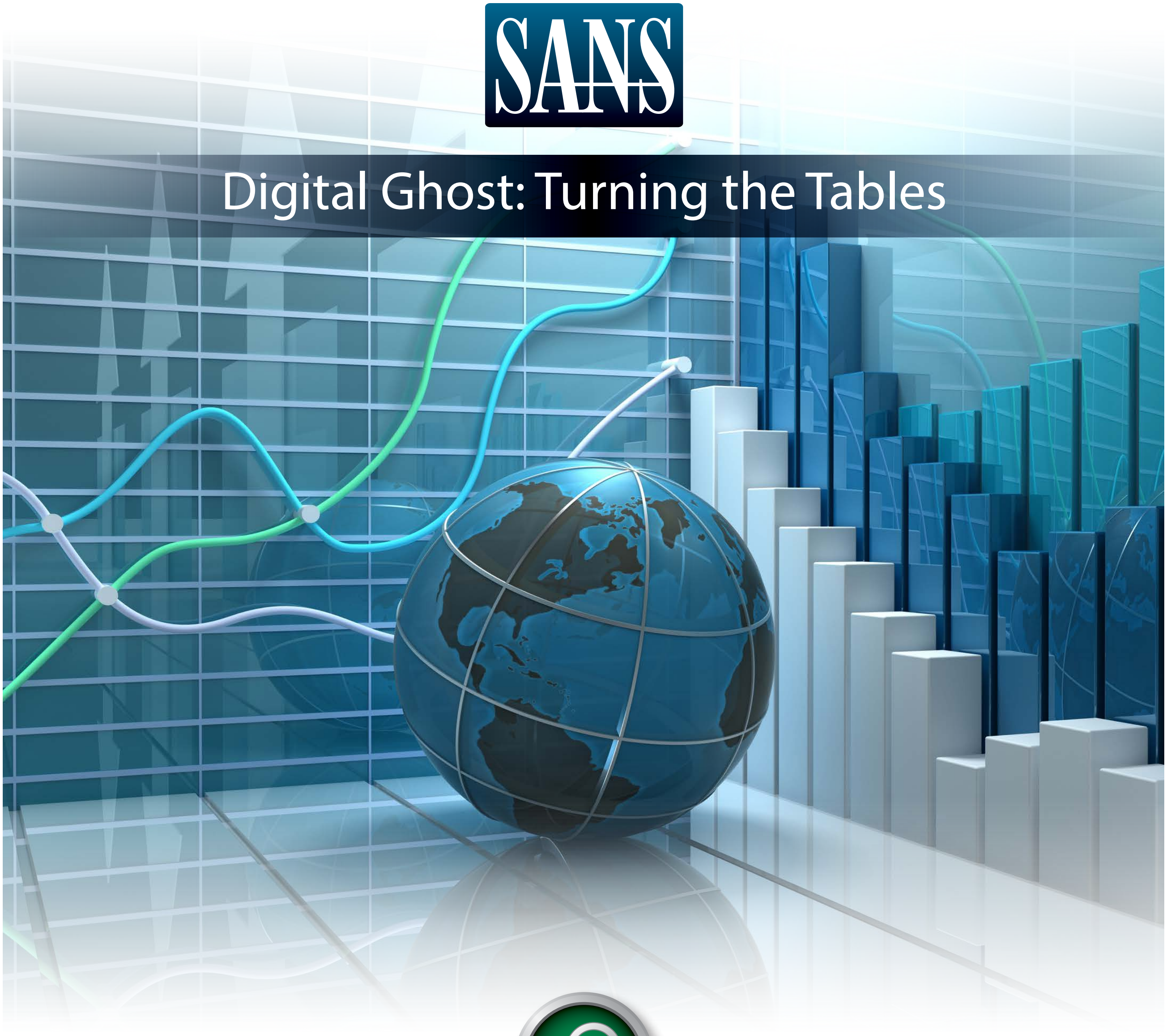
Digital Ghost: Turning the Tables

The complex weave of digital technology relies heavily on hyperconnected systems to move data and unlock value through analytics. The benefits are real, but the stakes involved require a serious look at the potential downsides, including the risk of cyber attacks. Organizations embracing technology innovation should not focus solely on efficiency and productivity, for innovation done correctly can also reduce the risks that come with expanding digital touchpoints.

Digital Ghost: Turning the Tables



A SANS Whitepaper

Written by Michael J. Assante

February 2017

Sponsored by
General Electric

Innovating Ahead of Highly Targeted Cyber Attacks

The dawn of pervasive game-changing automation is already upon us. The ability to harness data is letting us reinvent business models and streamline operations. The complex weave of digital technology relies heavily on hyperconnected systems to move data and unlock value through analytics. The benefits are real, but the stakes involved require a serious look at the potential downsides, including the risk of cyber attacks. Organizations embracing technology innovation should not focus solely on efficiency and productivity, for innovation done correctly can also reduce the risks that come with expanding digital touchpoints.

It is time for some deliberate and focused innovation to help turn the tables on cyber attackers, and industrial systems are poised to become the place where it happens. Industrial companies are transforming with the revelation that physics/process data and digital technology are important and valuable assets, alongside their large physical machines. This is a double-edged sword. As the industrial heart of the economy becomes more vulnerable to cyber attack, it might hold the answer to novel and powerful ways to protect organizations from high-consequence cyber risk. This paper provides new concepts for using ubiquitous sensing and reasoning to detect suspicious event occurrences, forming the basis for an adaptive machine response.

Innovation done correctly can reduce the risks that come with expanding digital touchpoints.

The simple idea is to use our deep knowledge of both the industrial process and the complex machines under control to devise a new way of sensing attacker experimentation or early actions when launching an attack. Defenders' greatest strength is their knowledge of the industrial processes and assets under their control. Together with their partners, defenders are often the creators of the chessboard on which a cyber contest is played to its conclusion. Designing and engineering the game board so it can inform you of the opponent's moves can turn the tables. As defenders, we can develop and deploy digital ghosts that hide translucently, are insubstantial to the machine, but are able to catch cyber attackers as they manipulate their targets.

Honestly, we have little choice but to innovate to gain an advantage over cyber attackers. We must move full circle because yesterday's world of electromechanical solutions that could not be controlled remotely is slipping away. These systems were complex but knowable, because we understood the modes of failure. Today's world includes a complex array of software-based devices that are highly networked to comprise a functional system with all sorts of features. We won't fully understand all modes of failure unless we invest in a deliberate effort to develop models and the necessary understanding of both the individual elements and the entire system-of-systems.

Tomorrow's world will likely require us to become much better in comprehending and managing our cyber exposures. If we don't, we will have to reject connections to the Internet and third-party networks for our critical infrastructure systems.

Lessons from recent cyber breaches provide us with the following security assumptions for the new normal:

1. Perimeter defenses are necessary in our attempts to keep intruders out, but they are insufficient.
2. You *will* be breached.
3. There is a high probability that you have already been breached.
4. Most organizations are unable to detect sophisticated intruders.
5. Intruders may compromise your system for more than a year before you are alerted to them.
6. You are more likely to be notified of an intrusion by a third party than discover it using your security technologies.
7. Intruder motivations can vary from gaining sustained access and stealing your secrets to launching highly disruptive or destructive attacks.

These are just a few of the reasons why some experts warn that attackers have a great advantage over defenders for the foreseeable future. Recent revelations of malware infections in well-protected, high-security-architected nuclear power plants demonstrate the shortfalls of a prevention-only security strategy.[1] This author recognizes these assumptions as mostly true but has a very different outlook for what the future holds.

[1] "German nuclear plant's fuel rod system swarming with old malware," April 27, 2016, http://arstechnica.com/security/2016/04/german-nuclear-plants-fuel-rod-system-swarming-with-old-malware

Flipping the Coin on Primacy

Targeted attacks with very real consequences are on the rise in energy infrastructures around the globe. The end of 2015 brought with it a very public cyber campaign that resulted in power disruptions and crippling attacks that impaired the Supervisory Control and Data Acquisition (SCADA) systems of three different distribution utilities in Ukraine.[2] The attackers proved adept at using power system automation to their advantage before launching a series of destructive attacks designed to deny use of these important tools in the restoration of power. The attacks were highly coordinated, well planned and synchronized to overwhelm system operators by using well-crafted and positioned attacks to have an impact on operational technologies in control rooms and numerous substations. This attack followed reports by Germany's Federal Office for Information Security [BSI], indicating that cyber attackers had intruded on a steel mill, exercised knowledge of its industrial control systems (ICS) and caused damage to a furnace under control.[3]

Today's attackers have demonstrated that they are goal oriented, expend intellectual energy to develop a plan, exercise patience and adapt to challenges they encounter in their target's systems.

These attacks illustrate the danger of allowing attackers access and intimate knowledge of our industrial processes. The challenge comes with our mutual realization that preventing all attacks is a fool's errand because attackers have become very good at finding mistakes or exploiting pervasive human weaknesses.[4]

Today's Defenses

A growing number of cyber attackers are continuing to hone their skills and applied learning to become very good at intruding upon our systems and burrowing deep enough to exercise their freedom of movement and action. These groups have demonstrated that they are goal oriented, expend intellectual energy to develop a plan, exercise patience and adapt to challenges they encounter in their target's systems. These habits, combined with the luxury of choosing their attack targets, places and times, have resulted in many experts declaring that attackers have a superior advantage. This is certainly true if the target is ill-prepared and does not anticipate and mitigate cyber attacks.

[2] "Analysis of the Cyber Attack on the Ukrainian Power Grid, Defense Use Case," March 18, 2016, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[3] "Die Lage der IT-Sicherheit in Deutschland 2014," www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile (Written in German.)

[4] "Verizon 2015 Data Breach Investigation Report," www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf

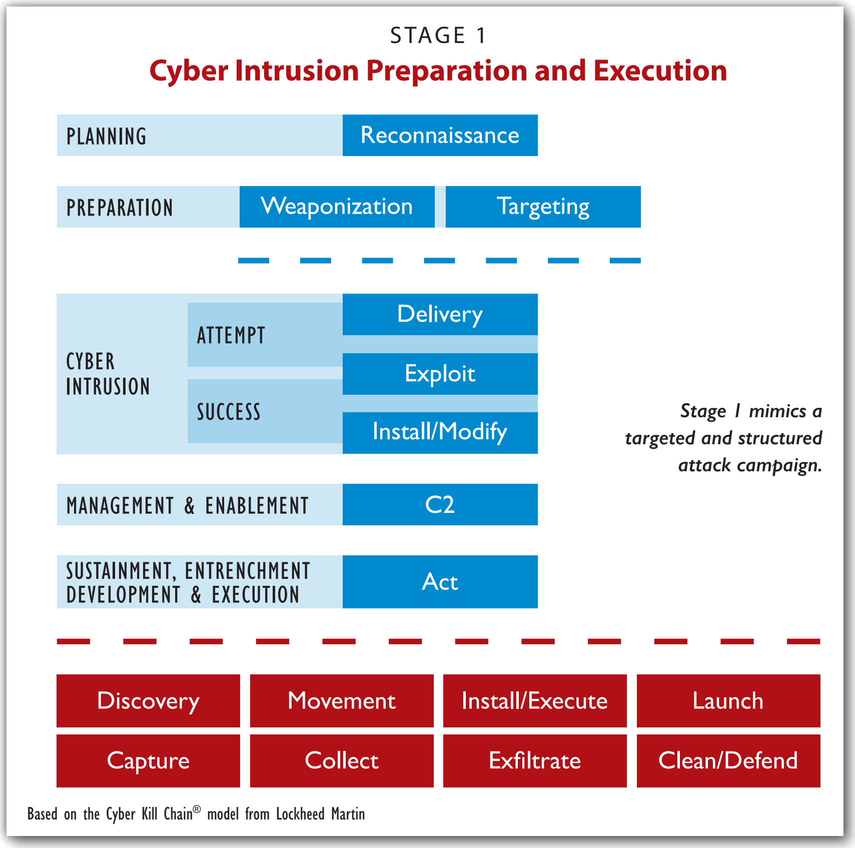
Leveraging the "intelligence" of the system can drastically increase the difficulty of planning and executing an impactful attack. Using cognitive learning engines or precise machine models, we can harness already existing instrument-derived measures to identify attempts to manipulate or change the process.

A defensible environment with well-trained defenders can make a contest of it, but we need to do more. As our reliance on digital technology grows, it comes with the imperative that defenders not only catch up with attackers but leap ahead of them to safeguard the value being created. Turning the tables requires maximizing the advantage of deep process, system and machine knowledge, and harnessing it to provide a labyrinth of unobservable sensors able to detect suspicious changes. Leveraging the "intelligence" of the system can drastically increase the difficulty of planning and executing an impactful attack. Using cognitive learning engines or precise machine models, we can harness already existing instrument-derived measures to identify attempts to manipulate or change the process. These techniques are already proving to be successful in advanced prognostic applications.

A quick example of a cognitive engine or the implementation of a more direct rule-based filter would allow an overwatch system that is monitoring system state to detect malicious operation of several remotely controlled circuit breakers over a short period of time. Power system operations other than Remedial Action Schemes (RAS) or Special Protection Schemes (SPS) rarely require opening circuit breakers rapidly across multiple substations. An overwatch system could have been used in the case of the Dec. 23, 2015, Ukraine SCADA hijacks to recognize and act on the highly suspicious behavior of multiple system dispatchers opening breakers throughout their parts of the system. If the system had incorporated a feedback loop to the front-end processor (FEP) or SCADA server, it could have nullified the commands before they were sent or might have diverted them to a sandbox for a supervisor's review. The implementation of such a system can be tricky. It could itself be used to cause an attack if an adversary could co-opt its capability.

Attack Models

By studying lab experiments and actual ICS attacks in which cyber actions resulted in process manipulation or damage to equipment under control, the SANS ICS team developed an attacker model to help inform defensive thinking. This model expands upon the traditional cyber kill chain developed by Lockheed Martin[5] by incorporating the necessary attacker steps to conduct an ICS-capable cyber attack. Stage 1 is illustrated in Figure 1.



Stage 1 mimics a targeted and structured attack campaign.

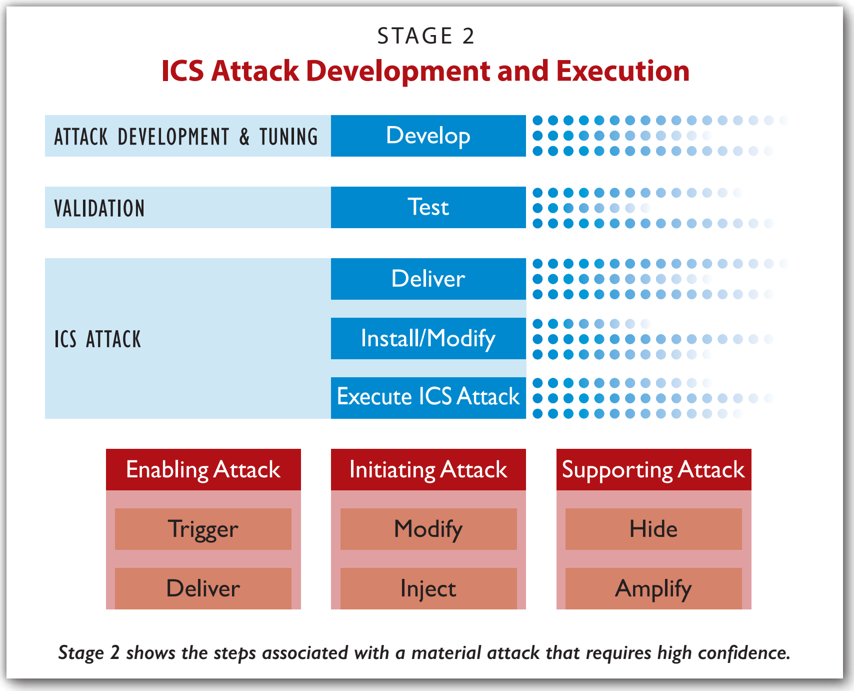
Based on the Cyber Kill Chain® model from Lockheed Martin

Figure 1. ICS Kill Chain Stage 1: Cyber Intrusion Preparation and Execution

This model can be described as an exaggerated kill chain that produces additional opportunities to detect and disrupt an ICS-focused cyber attack. The actors that are modeled here typically represent highly structured groups that have a role in influencing politics, economics and national security, and in stealing others' secrets. These groups are usually well resourced and have the ability to integrate multidisciplinary skills to plan and execute cyber operations.

[5] Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin, Ph.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

The second part of the ICS kill chain covers the development and execution of the attack. As is evident in Figure 2, attackers must have a variety of skills to successfully launch an attack against an industrial control system.



Stage 2 shows the steps associated with a material attack that requires high confidence.

Figure 2. ICS Kill Chain Stage 2: ICS Attack Development and Execution

Bridging the gap between Stage 1 and Stage 2 requires the attacker to gain both sufficient access and knowledge to devise a concept to operate against the industrial process or a machine under its control. This can be a complex and difficult undertaking and requires enough attacker free time (prior to detection) to maneuver into the necessary systems required to learn or attack in a way that can have an impact on the industrial process. This two-part kill chain means an ICS is inherently more defendable than an Internet-facing IT network. The SANS ICS team refers to this as an exaggerated kill chain that works in favor of a well-trained, prepared and active defender.[6]

The authors of the ICS Kill Chain had observed through years of experience and research, and by deconstructing real-world attacks on industrial processes, that predictable and material attacks often required multiple steps to achieve a result. Some attacks require actions to put the system into a condition in which attackers are able to initiate the actions required to achieve their goal. The initiating attack may also require a supporting attack to fool system operators long enough to achieve some necessary state change (for example, heating a liquid to a specific temperature to achieve a high enough pressure to cause damage).

[6] "The Industrial Control System Cyber Kill Chain," www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

The digital ghost concept, using measurements to detect process and machine changes, would look for sensing opportunities that go beyond traditional network or host-based security monitoring. The process, its instruments and actuators, and greater ICS should be analyzed by system designers/owners (e.g., ICS engineers) or original equipment manufacturers (OEMs) for particular machines and equipment to determine what sensing data defenders can use to identify attack experimentation, or actual attempts to change setpoints or provide dangerous commands out of sequence. Energy operational technology (OT) provides both in-system and instrument-provided data that can be pushed to cognitive learning engines to determine whether the observed measurements or actions are within a safe boundary for the process or are suspicious. The other unique advantage to using sensing is the ability to develop multiple sources to verify truth, which increases attacker complexity. Finally, data can be set up to be extracted in a manner that is difficult to see or anticipate, adding doubt and uncertainty for attack planners.

Defense in Depth

Engineering a digital ghost capable of analyzing data from an industrial process provides defenders with a solution that is:

- **Stealthy**—Makes a security system difficult to identify, circumvent and compromise
- **Proactive**—Actively looks for suspicious behavior
- **Detective**—Provides full-view, context-aware process monitoring, analysis and alerting
- **Adaptive**—Able to adapt as needed by using a cognitive engine or matching system applied to an accurate machine model

By using data that comes from the industrial process or from instruments tied directly to a machine under control, a defender can add a new dimension to achieving defense in depth (see Figure 3).

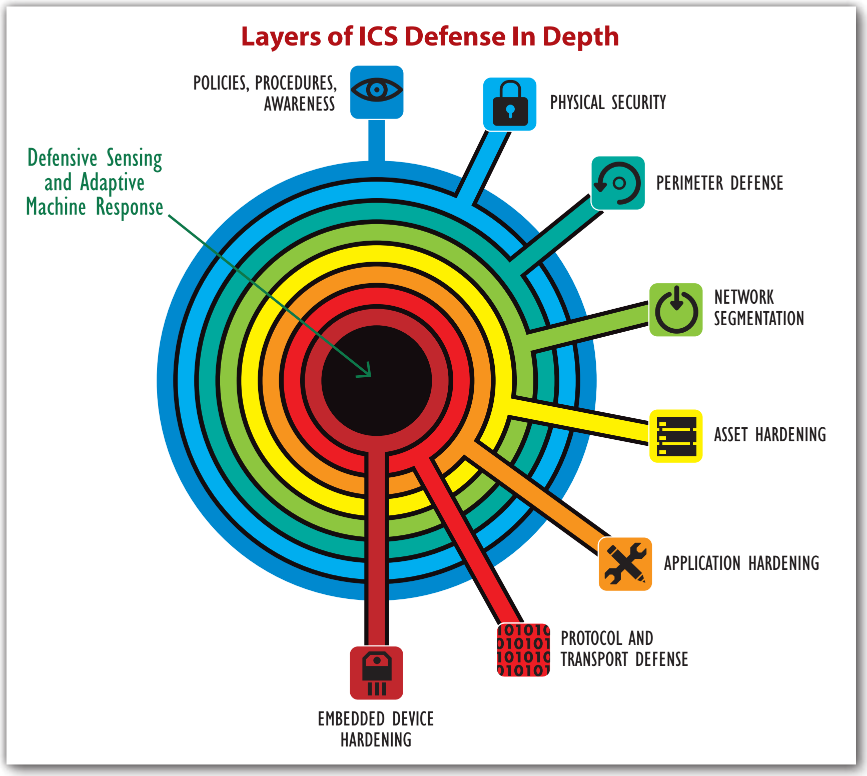

Layers of ICS Defense In Depth
POLICIES, PROCEDURES, AWARENESS
PHYSICAL SECURITY
PERIMETER DEFENSE
NETWORK SEGMENTATION
ASSET HARDENING
APPLICATION HARDENING
PROTOCOL AND TRANSPORT DEFENSE
EMBEDDED DEVICE HARDENING
Defensive Sensing and Adaptive Machine Response

Figure 3. Going Beyond Cyber Security to Achieve Multidimensional Defense in Depth

The process necessary to breathe life into a digital ghost requires a multidisciplinary team of process and machine experts and a logic or math engine to receive data and determine whether measurements indicate suspicious events.

The necessary steps include a mixture of engineering, networking, programming and testing:

1. Develop process and machine misuse cases.
2. Review existing instrumentation and measurements.
3. Consider additional instruments or sensors.
4. Review process and machine models.
5. Develop concepts for rule-based logic, cognitive learning algorithms and physics.
6. Design a model-based test system.
7. Consider determination outcomes (alerting or actions).
8. Design an architecture and network to collect the required data.
9. Implement the necessary hardware and software.
10. Conduct extensive testing.
11. Protect the new system and associated information.

Using Measurements Within a Turbine to Detect an Intrusion

Several misuse cases exist in which an attacker could manipulate a control and safety system to damage process or machine conditions. A modern power plant is composed of a balance of plant systems, the turbine and the generator. An attacker could use a number of approaches to introduce risk into these complex systems. Looking at a steam turbine, an attacker could focus on systems that provide the vacuum, enable cooling or moderate the steam entering the turbine.

The attemperator spray valves are controlled elements used to control the temperature, and therefore the quantity, of the steam entering the turbine. Improper operation of the valves could result in damage by reducing the temperature of the steam released, allowing too much water into the system. A cyber attacker could make sufficient changes to valve controls to reduce the temperature. However, turbine thermocouple measurements fed to an accurate machine model could detect even small changes. This technique could detect attackers' efforts to test whether they can have an effect.

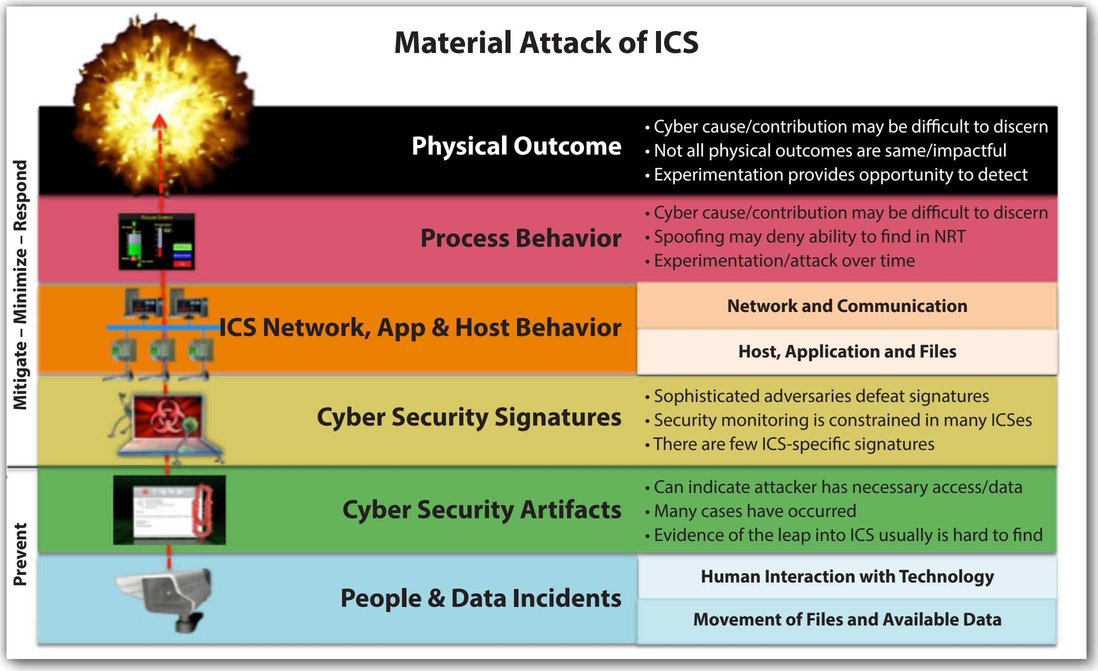
You can also use machine sensor data to identify malicious behavior on a gas turbine. These machines are susceptible to damage by having slight changes made to key control setpoints. One type of subtle attack involves slight adjustments to produce a rise in operating temperature. If unchecked, an attack of this nature is capable of removing significant life from the turbine in less than 12 months. By leveraging deep knowledge of how these machines operate, a defender can rely on machine sensors to provide an indication of pending damage. These cyber-enabled defensive techniques go beyond traditional information security to deliver deep insight that can't be observed by a would-be attacker.

Out-of-Band Detection

It is a powerful feat to have a detection system that lies out of reach or just out of the attacker's real-time perception. Passive taps provide us with the ability to collect data and leave the attackers wondering whether their actions are being observed or not. There are some architecture options where instruments can dual-report measurements to provide a method for sensing and analyzing data out of band from the targeted ICS (e.g., the production distributed control system used to operate the plant). These concepts can also be applied to a wide area system such as synchrophasors, where phasor measurements can be collected and analyzed to determine actions taking place on the power system. Trying to account for these measures would require an attacker to compromise the transmission SCADA system and the phasor system external to the utility to deny or spoof vital information that an attack is underway. Several universities and national labs have been looking at how to analyze phasor-derived data to identify system events and potential attacks on the system. The Defense Advanced Research Projects Agency (DARPA) has commissioned the Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program to detect attacks on the power system by analyzing system measures.[7]

[7] www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems

It is important to expand the layers of data used for the purposes of making security determinations. Higher levels of data usage may enhance the ability of defenders to secure their critical systems (see Figure 4).



Material Attack of ICS

Mitigate – Minimize – Respond

Prevent

Physical Outcome
- Cyber cause/contribution may be difficult to discern
- Not all physical outcomes are same/impactful
- Experimentation provides opportunity to detect

Process Behavior
- Cyber cause/contribution may be difficult to discern
- Spoofing may deny ability to find in NRT
- Experimentation/attack over time

ICS Network, App & Host Behavior
- Network and Communication
- Host, Application and Files

Cyber Security Signatures
- Sophisticated adversaries defeat signatures
- Security monitoring is constrained in many ICSes
- There are few ICS-specific signatures

Cyber Security Artifacts
- Can indicate attacker has necessary access/data
- Many cases have occurred
- Evidence of the leap into ICS usually is hard to find

People & Data Incidents
- Human Interaction with Technology
- Movement of Files and Available Data

Figure 4. Layers of Data that Can Be Used for Detection

Our current IT-centric cyber detection strategies rely on host- or network-provided data to make security decisions (filters, rules or heuristic determinations). A digital ghost would take data from the processes and machines under control to determine whether a malicious operator or programmer was trying to modify the process or equipment under control. This logic does not need to follow the boundaries we place on safety system configurations, which can rely on learning safe system envelopes or can be set to alert system operators if the safety system has been neutralized or changed by an attacker.

Adaptive Systems

Detecting a dangerous change to a real-time system is only half the battle. System designers must also decide whether simple engineering and operator alerts are sufficient or whether a particular event might require an automatic machine-calculated response. Those interested in developing such a system must carefully consider and test the implementation of an adaptive system that can act without the permission of a human. We don't want to introduce another mechanism for an attacker to hijack for malicious purposes. There are a few approaches to harnessing information from a digital ghost system to provide predefined commands back to the distributed control system (DCS) or machine that puts the system in a more conservative state or initiates a safe shutdown procedure to minimize the potential for damage. As an example, a physically separate system that sits behind two-way unidirectional security gateways may provide a good-enough solution that would introduce a tremendous amount of difficulty to an attacker. First, the system would be hard to identify and comprehend from inside the breached system. Second, the amount of effort needed to compromise the system would increase the overall energy and resource requirement for a successful attack.

A common attacker tactic is lying inside a modern ICS. This type of attack can be difficult if it has to be carried out in too many places. Consider the lying used in the replay attack by Stuxnet to create a false view of the process under control. A system recording was replayed back to the human machine interface (HMI) showing enrichment processes operating under normal conditions, while the actual attacks were changing measurements as machines under control were being damaged.[8,9] An adaptive system could trigger upon detection of an inconsistency in data or an attempt to lie and initiate a safe system shutdown or isolate sections of the control system. Adaptive systems can analyze and take appropriate actions based on measurements or inconsistencies between sensor readings and reported conditions.

[8] Kim Zetter. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Broadway Books: New York, reprint edition, 2015.

[9] "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Acieve," Ralph Langner, November 2013, www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

Conclusion

Every automation system owner should be striving to reduce complexity and unwieldy or poorly implemented system integration. The hallmark of a highly reliable system is for engineers and operators to possess a comprehensive understanding of how that system operates and what constitutes expected behavior and normal communications. Great opportunities exist to reduce unplanned events and devise schemes to detect system manipulations before they result in difficult-to-recover-from consequences. These techniques may add an element of surprise and tip the balance of power in the defender's favor. By thinking beyond network and hosts, defenders can reach into the actual ICS and machines to harness existing process data for security monitoring. Those with a deep understanding of their systems and physical assets, plus the value of adaptive model-based control, should consider implementing concepts such as the digital ghost.

Leadership in today's digital market favors those who can see beyond the immediate application of any specific solution to drive greater systemic value, all while addressing the inherent risks that come with a smaller, more connected world. Let's innovate a brighter and more secure future where critical industrial and infrastructure systems are much more than hard-to-defend targets. Our future systems and machines will be smart enough to help defenders detect intruders, and they will adapt to minimize damages.

About the Author

Michael Assante currently manages the SANS Industrials and Infrastructure practice area and is the lead for the Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) security curriculum. Previously he served as vice president and chief security officer of the North American Electric Reliability Corporation (NERC), where he oversaw industrywide implementation of cyber security standards across the continent. Before joining NERC, Mike held a number of high-level positions at Idaho National Laboratory and served as vice president and chief security officer for American Electric Power. His work in ICS security has been widely recognized.

Sponsor

SANS would like to thank this paper's sponsor:

Last Updated: March 8th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Secure Singapore 2017	Singapore, SG	Mar 13, 2017 - Mar 25, 2017	Live Event
SANS Secure Canberra 2017	Canberra, AU	Mar 13, 2017 - Mar 25, 2017	Live Event
ICS Security Summit & Training - Orlando	Orlando, FLUS	Mar 19, 2017 - Mar 27, 2017	Live Event
SANS Tysons Corner Spring 2017	McLean, VAUS	Mar 20, 2017 - Mar 25, 2017	Live Event
SANS Abu Dhabi 2017	Abu Dhabi, AE	Mar 25, 2017 - Mar 30, 2017	Live Event
SANS Pen Test Austin 2017	Austin, TXUS	Mar 27, 2017 - Apr 01, 2017	Live Event
SANS NetWars at NSM Security Conference	Oslo, NO	Mar 28, 2017 - Mar 29, 2017	Live Event
SEC564: Red Team Ops	Atlanta, GAUS	Apr 06, 2017 - Apr 07, 2017	Live Event
SANS 2017	Orlando, FLUS	Apr 07, 2017 - Apr 14, 2017	Live Event
Threat Hunting and IR Summit	New Orleans, LAUS	Apr 18, 2017 - Apr 25, 2017	Live Event
SANS Baltimore Spring 2017	Baltimore, MDUS	Apr 24, 2017 - Apr 29, 2017	Live Event
SANS London April 2017	London, GB	Apr 24, 2017 - Apr 25, 2017	Live Event
Automotive Cybersecurity Summit	Detroit, MIUS	May 01, 2017 - May 08, 2017	Live Event
SANS Riyadh 2017	Riyadh, SA	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CAUS	May 09, 2017 - May 18, 2017	Live Event
SANS Zurich 2017	Zurich, CH	May 15, 2017 - May 20, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VAUS	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, GB	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, AU	May 22, 2017 - May 27, 2017	Live Event
SANS Madrid 2017	Madrid, ES	May 29, 2017 - Jun 03, 2017	Live Event
SANS Stockholm 2017	Stockholm, SE	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GAUS	May 30, 2017 - Jun 04, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS London March 2017	OnlineGB	Mar 13, 2017 - Mar 18, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced