Stuxnet to CRASHOVERRIDE to TRISIS: Evaluating the History and Future of Integrity-Based Attacks on Industrial Environments

Joe Slowik, Dragos

Executive Summary

Industrial Control System (ICS) attacks are typically viewed as immediate disruptive events designed to directly impair, damage, or otherwise disrupt an industrial process. Yet an analysis of the most significant ICS security events to date – Stuxnet, CRASHOVERRIDE, and TRISIS – reveals more worrying ambitions. Rather than seek immediate disruption, each of these attacks sought to undermine a fundamental aspect of process integrity as part of a multi-staged intrusion event to achieve impacts far greater than simply shutting down a plant or stopping the flow of electricity.

By appreciating and understanding this nuance in past events, ICS asset owners and defenders can gain greater understanding of potential ICS attack vectors – and the appropriate responses to attacks that seek to undermine critical aspects of operational environments. Most importantly, nearly all such attacks feature at least some degree of impact on process protection or safety, resulting in potentially hazardous process conditions (and physical destruction) either through the attack lifecycle, or when a compromised process is restored without understanding (or even knowing) it has been changed.

Given these developments in the ICS attack landscape, asset owners and operators must embrace more robust defensive measures to identify and respond to such attacks. Direct identification of attack vectors through IT-centric monitoring or network-based anomaly detection will produce a weak signal for investigation in most instances, where such techniques even alert operators at all. Instead, asset owners must adopt practices to fuse multiple data sources together to produce ICS-centric, contextual alarms keyed to ICS risk and adversary behavior. The central focus of such efforts must be identification of root incident cause, and then determining incident implications, to adequately deal with threats that seek to undermine fundamental aspects of industrial environments. Furthermore, security investment does not stop at detection but rather extends to remediation and recovery. Identifying needs relative to attacker tradecraft and objectives now ensures defenders are best-positioned for future scenarios that seek to cause damage in industrial environments.

Table of Contents

Introduction

Industrial control system (ICS) cyber intrusions range in purpose from initial access to data gathering to industrial espionage to process disruption and physical destruction. Although the continuum of possible events is quite broad (See Table 1), the number of publicly known, ICS-focused events remains relatively small as of this writing. As a consequence of this small sample size, popular conceptions of ICS events typically label all such incidents as “attacks” while avoiding or ignoring the nuances of differentiating events, their likely purpose, and probable impact scenarios.

Table 1: ICS Attack Types and Examples

	Survey & Reconnaissance	Theft & Monetization	Disrupt & Destroy
Purpose	• Gather ICS-related information • Establish points of access in ICS networks	• Gather trade secrets or economically-valuable information • Leverage ICS criticality for extortion or ransom	• Deny, degrade, or destroy ICS operations • Cause process-disruption or physical destruction
Examples	• ALLANITE[1] • DYMALLOY[2] • Dragonfly[3]	• Ryuk, Lockergoga[4]	• Stuxnet[5] • 2015 Ukraine[6] • CRASHOVERRIDE[7] • TRISIS[8]

While the above summarizes observed events and adversary goals in executing them, the table avoids a critical aspect of ICS events: process impact. Typically, when measuring impact and the goals of security, IT security professionals refer to the “CIA Triad” comprising: confidentiality, integrity, and availability[9]. When shifting from IT to ICS networks, security practitioners typically emphasize scenarios impacting availability – most notably the destructive items in the final column in Table 1. Yet this emphasis on availability exclusively ignores potentially disastrous scenarios involving different types of security impacts.

[1] ALLANITE - Dragos
[2] DYMALLOY – Dragos
[3] Dragonfly: Cyberespionage Attacks against Energy Suppliers – Symantec
[4] Implications of IT Ransomware for ICS Environments – Joe Slowik, Dragos
[5] Win32.Stuxnet Dossier – Nicolas Falliere, Liam O Murchu, and Eric Chien, Symantec
[6] Analysis of the Cyber Attack on the Ukraine Power Grid – Robert M. Lee, Tim Conway, Mike Assante (SANS Institute and E-ISAC)
[7] Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE – Joe Slowik, Dragos (Virusbulletin 2018)
[8] TRISIS Malware – Dragos
[9] The CIA Triad – The Infosec Institute

This paper seeks to analyze one specific, concerning type of attack scenario on ICS networks: intrusions that aim to undermine the integrity of industrial processes to produce a malicious functional impact. While the overall number of publicly-identified ICS-related events remains small[10], and the number of actual attacks smaller still, the proportion of the most serious events which aim (or sought) to undermine process integrity is outsized compared to more simplistic scenarios such as direct disruption. Furthermore, the nature of integrity-focused attacks requires a different mindset and operational playbook for defense and recovery compared to direct, immediately impactful attacks popularly conceived as the primary goal of cyber-physical events.

The following paper will seek to define attacks and ICS process requirements to achieve clarity in discourse, then proceed to review previous, high-profile ICS attacks – Stuxnet, CRASHOVERRIDE/Industroyer[11], and TRISIS/Triton[12] – to explore how each of these represented a fundamental attack on underlying process integrity as opposed to more popularly-conceived direct disruption. Based on these observations, this paper will then explore possible future scenarios seeking similar impact across ICS industry verticals to illustrate the risk of such events, while also highlighting requirements and recommendations for defense and recovery.

Defining ICS Attacks

An unfortunate trend in information security reporting overall, and ICS-focused security coverage in particular, is overuse and abuse of the word “attack.” Events as disparate as external network scanning, espionage, ransomware, and truly disruptive operations all get lumped together in much public discourse as constituting “attacks”. Yet this overly-broad conception hides nuance lying behind each of these event types and serves to deaden us to the true meaning and impact of actual disruptive events.

For this paper, “attack” is narrowly defined to encompass only those actions that deny, degrade, or destroy either an IT system, ICS system, or a physical process controlled by such a system through cyber-nexus means[13]. Of note, preparatory actions – such as direct reconnaissance or access operations – can be construed as attacks so long as adversary intent is to take the knowledge or access gained to further a future offensive event. Within the context of US military language and doctrine, this is frequently referred

[10] Dragos incident response activity includes a large number of intrusions that have never been revealed publicly. Presumably, other ICS security providers have similar experiences. Thus, the absolute number of ICS intrusions is likely far larger than publicly-available data would indicate.

[11] Win32/Industroyer – A New Threat for Industrial Control Systems – Anton Cherpanov, ESET

[12] Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure – Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, and Christopher Gloyer, FireEye

[13] Derived from: NSA/CSS Technical Cyber Threat Framework v2 – National Security Agency/Central Security Service, and US Department of Defense Joint Publication 3-13 – Information Operations – US Joint Chiefs of Staff

to as “operational preparation of the environment.”[14] While useful and reflecting experience, this paper will treat such items as out of scope due to both lack of necessary information (gauging likely adversary intent before an executed attack) and irrelevance to our limited set of events (looking for items that actively sought to undermine process integrity, rather than merely desiring to do so).

While later sections of this paper will explore potential scenarios for process integrity-based attacks that may be enabled by currently-active initial access and reconnaissance operations (most notably on-going “Dragonfly2.0” or ALLANITE activity with respect to western electric utility operations[15]), this will be a theoretical examination of impact possibilities. Our focus will be on what constitutes an actual, deployed, integrity-based attack within industrial environments.

ICS Attack Value and Operational Integrity

Attacks on ICS networks can map to different aspects of the CIA triad, seeking to undermine:

CONFIDENTIALITY: The security or privacy of privileged or sensitive information.

INTEGRITY: The fundamental soundness and non-alteration of a given system, function, or data.[16]

AVAILABILITY: The accessibility and presence of the necessary system or function within operations.

[14] 'Operational Preparation of the Environment': 'Intelligence Activity' or 'Covert Action' by Any Other Name? – Joshua Kuyers

[15] Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group – Symantec; Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors – US-CERT; Electric Sector Targeting in Context – Joe Slowik

[16] For the purposes of this paper, process safety is a component of overall process integrity. While not perfect, this conception adequately identifies the nature of safety (a known-good, known-safe process state) within the existing CIA framework.

Each of these is important for operations, and all have a role in ICS functionality. Industrial environments that cannot keep data confidential risk losing important trade secrets and related information to competitors or other entities. Loss of availability means that a given plant environment is unable to function or perform its designed task. But integrity has a special place in ICS operations given the physical nature of the underlying processes controlled by ICS devices, and the implications behind modifying a process such that its integrity and results can no longer be accurately predicted.

Many entities and even best-practice guidelines for industrial security (such as ISA–62443-2-1[17]) emphasize availability as the most significant item in terms of risk and preservation.[18] Yet in industrial environments, integrity means that a given process, system, or even an entire plant has operations that remain in a known-good, known-safe state as designed and implemented when the process started. Deviations from this baseline require testing and verification to determine that underlying integrity – in terms of production accuracy but also process safety and reliability – is maintained. Given the centrality of known-good, verified process integrity, threats to this aspect of ICS security can be looked at as at minimum equivalently serious to the popular conception of availability concerns, if not more so given safety implications.[19]

To put the above succinctly, while plant owners are invested in ensuring that a plant can start or continue to run, no sane or safety-conscious individual would willingly embrace a process that they cannot stop. In this sense, the ability to ensure process accuracy, protection, and fundamental safety are critical requirements which cannot be dismissed or minimized.

Of note, an availability-focused attack is direct and obvious in nature. By virtue of execution, operators cannot access systems, or processes cannot function or produce. This represents a form of direct disruption, ranging from stopping production in a factory to cutting the flow of electricity. Conversely, an integrity attack is nearly always more indirect in nature and effect. Rather than directly disrupt or disable the process, an integrity-based attack seeks to subtly manipulate or alter process fundamentals in such a way as to increase the likelihood of or precipitate an undesired event. This end-goal may be disruptive in nature but will in almost all circumstances manifest itself only after the actual intrusion responsible for delivering it, and given the timing disconnect will be significantly harder to identify and diagnose as a cyber-physical attack.

[17] ISA-62443-2-1-2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program – International Society of Automation

[18] Examples of guidance stressing availability include: Incident Response for Industrial Control Systems – Chris Sistrunk, FireEye; Defending ICS Networks against Cyber Attacks with Better Log Correlation – Harry Thomas, Forescout; What is ICS Security? – Chris Brook, DigitalGuardian

[19] SCADA Security Basics: Integrity Trumps Availability – Eric Byres, Tofino Security

Review of Past Attacks

While there have been numerous intrusions into control system networks, there have been only a handful of publicly-known, deliberate ICS attacks (as defined above) at the time of this writing: Stuxnet, Ukraine 2015, Ukraine 2016 (CRASHOVERRIDE/Industroyer), and the Triton/TRISIS event in 2017.[20] Of these, Ukraine 2015 stands apart as a straight-forward disruption event with an emphasis on manual interaction with control systems to induce an outage, and then deploying follow-on malware to delay recovery. The remaining three represent something else entirely: leveraging purpose-built software as part of multi-stage attacks to undermine system integrity to produce not just process disruption or interruption, but either potential physical destruction or coordinated influence against process owners.

While the nature of these three events – Stuxnet, CRASHOVERRIDE, and TRISIS – means that precise forensic data and victim environment information are publicly unavailable, sufficient evidence exists (including malware samples) to analyze how these attacks were executed and to determine most-likely attacker intentions. Combined with public reporting and related information, we can reconstruct a reasonable representation of events to analyze attacker intentions and goals given deployed tools and their functionality.

Although all three cases appear to have received sufficient past attention and analysis, in each case events were primarily analyzed from the perspective of direct, immediate disruption to operations. As such, past analysis missed important implications on the true nature and desired impact of these events. Given this outlook and the framework described previously, the three headline ICS attacks will be reviewed to demonstrate how each ultimately reflects a fundamental attack on ICS integrity, whether to undermine process confidence (Stuxnet), protection (CRASHOVERRIDE), or safety (TRISIS).

STUXNET[21]

Stuxnet first emerged in the public conscious when Sergey Ulasen, then an analyst at Belarussian antivirus firm VirusBlokAda, identified a unique malware sample in company telemetry.[22] Following initial discovery, multiple teams from different organizations – including malware analysts at Symantec and ICS specialists at Langner Group – dug further into the mysterious malware to determine its function and purpose. Following initial, ultimately incorrect suppositions that the ICS-targeting malware was aimed at Iran’s Bushehr nuclear power plant,[23] analysts and researchers at several organizations

[20] One additional item often cited is a destructive event at an unnamed German steel mill in 2014 tied to a cyberattack. While concerning, insufficient evidence is available to discuss this event in detail, and thus this example is left out of this paper. For further information, see: German Steel Mill Cyber Attack – Robert M. Lee, Michael J. Assante, and Tim Conway, SANS Institute

[21] For in-depth coverage of Stuxnet’s investigation, purpose, and implications, readers are highly encouraged to examine Kim Zetter’s Countdown to Zero Day.

[22] How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History – Kim Zetter, Wired

[23] Stuxnet Logbook, Sep 16 2010, 1200 Hours MESZ – Langner Group

identified Iran's uranium enrichment operations at Natanz as the likely target.[24] In addition to the in-depth research performed by analysts at Symantec and Langner Group,[25] the overall nature of Stuxnet was at this point revealed: a very deliberate attack on the nuclear enrichment activities of Iran performed with a complex, purpose-built set of malware.

Yet the popular conception of Stuxnet relied upon a rather simple view of this malware's function: that when deployed, Stuxnet destroyed the centrifuges used in gaseous diffusion operations to enrich uranium hexafluoride.[26] While it was true that centrifuges were destroyed, the manner and observable nature in how this was achieved obscures the true significance of Stuxnet's impact. Rather than simply cause centrifuges to destroy themselves after infecting the relevant control system devices, Stuxnet performed a more subtle action: causing centrifuges controlled by an infected Siemens programmable logic controller (PLC) to alternate between operational extremes, in short timeframes and spaced in time, to ensure overall operational degradation. This impact is significantly different from a direct disruptive or destructive event in that it took time for affected centrifuges to wear out – in a manner that was difficult to diagnose and resulted in overall loss of confidence in the enrichment program.

Looking at various Stuxnet payloads, researchers identified two distinct variants: one to cause an extremely difficult to detect over-pressure condition in impacted centrifuges, the other to alter rotating speeds between extremes. Critically important in both attack types was that either mechanism can be used to directly and immediately destroy or disable centrifuges controlled by the infected PLC. Yet instead of going for direct disruption and destruction, Stuxnet's authors sought a far more nuanced impact. By moving centrifuges beyond normal operational tolerances for periods of time then restoring "safe" settings, Stuxnet worked to increase the defect rate and decrease the operational life of impacted centrifuges.

Operational stress inducement served an immediate purpose, but was paired with an additional functionality within Stuxnet: creating a loss of view condition on process telemetry during the attack sequence, particularly for the rotation speed attack. This served two related functions: first and most obviously, to reduce the likelihood of Stuxnet's detection when centrifuge operational parameters exceeded norms; second and more insidiously, to hamper process analysis and recovery operations by masking all relevant data from engineers attempting to diagnose the increased failure rate. The latter may seem a mere extension of the former, but in application is far more powerful as it introduces a significant level of doubt into plant operations. Namely, centrifuges begin to fail, but for reasons that cannot be discerned and for which no data is available. As reported publicly, "the Iranians had grown so distrustful of their own instruments that

[24] Stuxnet: Targeting Iranian Enrichment Centrifuges in Natanz? – Frank Rieger, Knowledge Brings Fear (blog); Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment – David Albright, Paul Brannan, and Christina Walrond, Institute for Science and International Security

[25] Win32.Stuxnet Dossier – Nicolas Falliere, Liam O Murchu, and Eric Chien, Symantec; To Kill a Centrifuge – Ralph Langner, Langner Group

[26] Uranium Enrichment – United States Nuclear Regulatory Commission

they had assigned people to sit in the plant and radio back what they saw."[27] Thus, we can look at Stuxnet – without even considering its propagation and infection mechanisms – as a multi-stage ICS attack: first creating a loss of view condition to inhibit analysis and process control, then following this with a loss and manipulation of control event to begin damaging enrichment equipment.

Based on these details, the destruction of a number of centrifuges was simply a means to an end: increasing uncertainty and decreasing confidence in the technical capability of Iranian uranium enrichment operations, producing policy and procedural changes that in the immediate term reduced the output of enriched fuel,[28] but more broadly provided enhanced costs to the Iranian regime for pursuing its nuclear program. As reported in subsequent analysis, Stuxnet formed one part of an overall strategy – called "Olympic Games" – that was designed to "set [Iran's nuclear program] back for a while to buy time for sanctions and diplomacy to take effect."[29] Thus, the goal of Stuxnet was not to destroy the Iranian nuclear program outright, but rather to impair and degrade it to foster doubt and create space for potential diplomatic solutions.

Context is critical in evaluating Stuxnet's deployment and effectiveness: the Natanz plant, operational since 2006, started its life using the Iranian-manufactured IR-1 centrifuge, based on the Pakistani P-1 with plans obtained via the A. Q. Khan proliferation network.[30] The P-1 was a legacy design prone to problems, with the IR-1 featuring even more reliability issues since its initial deployment.[31] Thus, Stuxnet (which may have been deployed as early as 2007) entered an environment already containing significant doubt and unreliability in operations. Essentially, Iranian officials took a risk in using a known-inferior device to attain strategic goals – but with assumed knowledge of the IR-1 failure rate to make appropriate, risk-based decisions.

By increasing the failure rate of the deployed centrifuges at Natanz, Stuxnet cast doubt on the previous decisions and calculations made by leadership as to the integrity and cost of the enrichment project. Given time, resource constraints, and the need to rely on either indigenous manufacturing or a trickle of black market-obtained equipment, increasing the perceived failures of enrichment operations (and potentially casting doubt by association to planned follow-on centrifuges to the IR-1) could work to powerfully alter the decision-making of Iranian leadership. Notably, Iran pursued extensive additional enrichment operations aside from the widespread use of the IR-1 at Natanz, including the construction of additional enrichment facilities at Fordow and an extensive development program to build successors to the IR-1.[32] Stuxnet did not target these

[27] Obama Order Sped Up Wave of Cyberattacks Against Iran – David Sanger, The New York Times
[28] Iran's Nuclear Program Suffering New Setbacks, Diplomats and Experts Say – Joby Warrick, The Washington Post; Iran Nuke Enrichment Sees Setback, Sources Say – George Jahn, Associated Press
[29] Revealed: How a Secret Dutch Mole aided the U.S.-Israeli Stuxnet Cyberattack on Iran – Kim Zetter and Hulb Modderkolk, Yahoo News
[30] Iran's Advanced Centrifuges – David Albright and Christina Walrond, Institute for Science and International Security
[31] Performance of the IR-1 Centrifuge at Natanz – David Albright and Christina Walrond, Institute for Science and International Security
[32] The Fordow Enrichment Plant, aka Al Ghadir: Iran's Nuclear Archive Reveals Site Originally Proposed to Produce Weapon-Grade Uranium for 1-2 Nuclear Weapons per Year – David Albright, Frank Pabian,

programs, but confidence in their efficacy would by association be lowered (and requirements for operational security and maintenance increased) as part of a coordinated, multi-discipline information operations attack against the Iranian nuclear program under Olympic Games. Essentially, Stuxnet's destructive behavior was simply a means to an end for altering Iranian leadership assessments as to the viability and utility of their nuclear enrichment program.

While Stuxnet was successful in the sense that it impacted centrifuges as designed, its exact efficacy given likely mission profile and the environment it was deployed to is unknown. As stated above, Stuxnet was discovered and publicly disclosed while still operating, thus providing decision-makers within the Iranian enrichment program a reason for the increased failure rate at Natanz. Yet had this discovery not occurred, the potential impact would not have been destroying the Iranian nuclear program, but rather decreasing its reliability and increasing its costs. Potential outcomes from this attack on fundamental process integrity could range from bleeding Iran of resources to produce and develop more equipment to maintain an uncertain enrichment process, or even provide an inducement for negotiations to give up the program due to increasing costs. In either event, Stuxnet was built for very specific purposes: to target a very small subset of industrial control equipment and to cause just enough damage to impair the overall process but not outright destroy it.

CRASHOVERRIDE/INDUSTROYER

CRASHOVERRIDE, also referred to as Industroyer, was a purpose-built, semi-modular malware framework used during the 2016 Ukraine power event.[33] Upon initial observation, the CRASHOVERRIDE event appeared superficially similar to the 2015 Ukraine incident in that electric utility operations were disrupted for several hours followed by actions to inhibit recovery at the infected utilities. Yet even on initial analysis, the two events diverge. While the 2015 incident focused on electric distribution operations and achieved disruption via manual interaction with control systems at the impacted locations,[34] the 2016 event targeted electric transmission operations and produced its ICS effects by encoding process manipulation in purpose-built software.[35]

The above, initially observed changes represent an evolutionary step in electric utility attack execution. By encoding ICS manipulation in software, CRASHOVERRIDE enabled a more efficient, larger scale operation than would be possible following the same methodology as 2015. Yet while this aligns with observed impacts, a closer analysis of how the CRASHOVERRIDE attack was executed and the latent (if in many cases non-functional) capabilities of tools used in the event reveals a far more ambitious and

and Andrea Stricker, Institute for Science and International Security; Iran's Long-Term Centrifuge Enrichment Plan: Providing Needed Transparency – Institute for Science and International Security

[33] CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations – Dragos; Win32/Industroyer – A New Threat for Industrial Control Systems – Anton Cherpanov, ESET

[34] Analysis of the Cyber Attack on the Ukraine Power Grid – Robert M. Lee, Tim Conway, Mike Assante (SANS Institute and E-ISAC)

[35] Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE – Joe Slowik, Dragos (Virusbulletin 2018)

potentially revolutionary attack sequence: a multi-stage event designed to cause potential physical destruction via a loss of protection on impacted systems.

CRASHOVERRIDE's extended ambitions first came to light publicly in August 2019 through a reassessment of attack artifacts and capabilities.[36] Based on an analysis of built-in capabilities in multiple artifacts related to CRASHOVERRIDE's deployment within the victim environment, several important details emerged: First, the intended scale of the transmission outage was far greater than what was actually achieved, with hundreds of systems targeted to attempt a complete shutdown of transmission operations at the impacted site. Second, the sequencing of events in the environment resulted in disabling control and SCADA systems in the environment, which produced a loss of view and loss of control event in addition to inhibiting recovery. Third and finally, the Siemens SIPROTEC protective relay denial of service (DoS) attack during the event was not a mere "throwaway" to make restoration more difficult, but a very deliberate attempt to leverage a particular vulnerability to eliminate transmission protection.

Comparison to the 2015 event is helpful, because it appears attackers in 2016 learned from the previous event. First, in 2015, Ukrainian operators quickly moved to restore service through manual intervention, even while SCADA equipment was essentially disabled for months due to the wiper deployed after interrupting distribution. Knowing this operational preference, deploying a wiper mechanism again in 2016 seems redundant except to produce long-term pain – but informs the attacker of what type of environment Ukrainian operators are likely willing to operate in to restore service. Thus, the wiper component in 2016 takes on a more interesting role: removing visibility into the functionality of the SCADA environment during an emergency as control systems become unresponsive and not useful.

[36] CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack – Joe Slowik, Dragos

Meanwhile, in the rush to restore interrupted transmission operations, the attackers deploy a denial of service against Siemens SIPROTEC protective relays in the environment using a publicly disclosed vulnerability. Modern, digital protective relays provide a mechanism to quickly react to changes in electric utility operating environments such that when a fault or other adverse condition arises, equipment can be disengaged or otherwise protected to prevent potential damage.[37] The specific vulnerability used during CRASHOVERRIDE places the vulnerable SIPROTEC device into a "firmware update mode."[38] Of note, the impacted device remains powered on and network accessible, and at cursory glance (e.g., while responding to a massive power disruption and frantically attempting to restore operations) may appear to be functional, shown in Figure 1.[39] Yet after delivery, all protection logic is removed from the device, meaning that any lines under the relay are no longer protected from potential fault or other hazardous conditions.

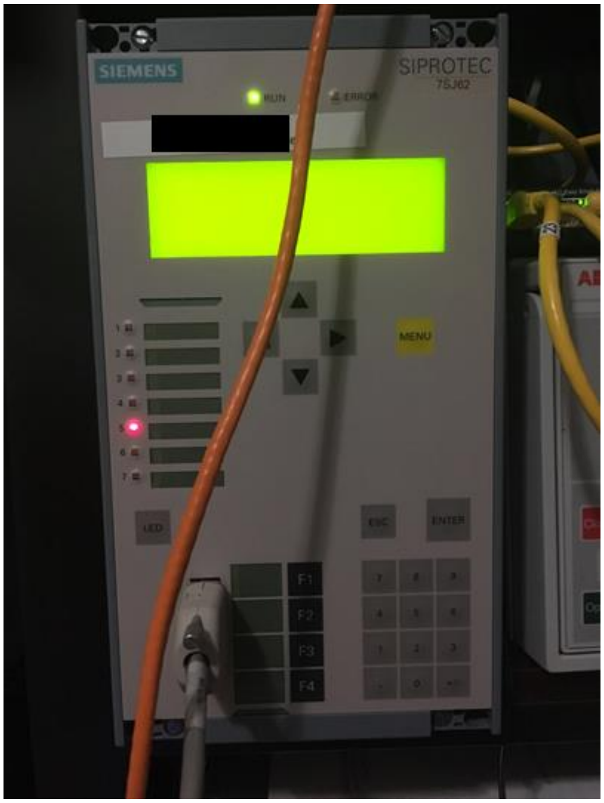
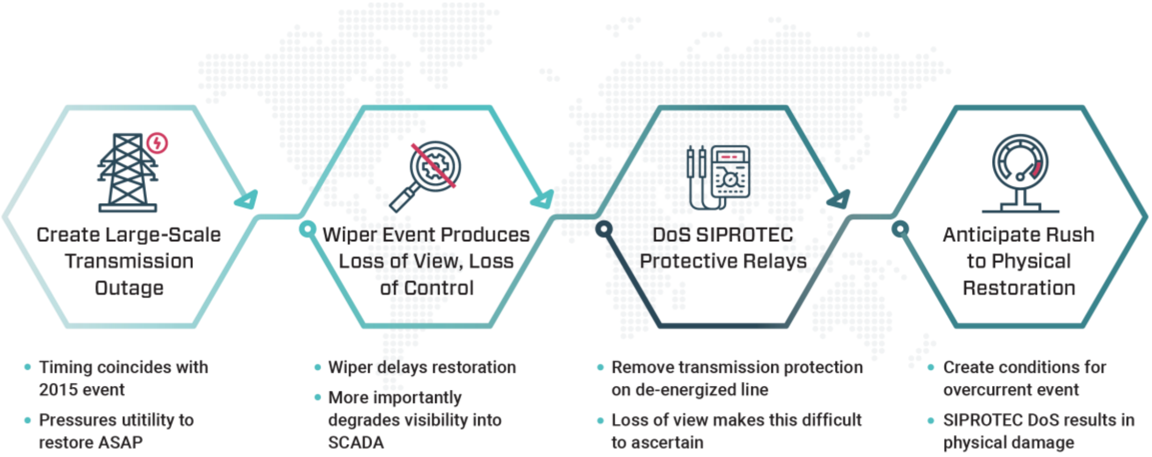


Figure 1: Siemens SIPROTEC Following DoS Execution[39]

Removing protection from a deenergized line at first appears nonsensical and pointless – until realizing, based on a study of the 2015 attack, that operators would be able and willing to reconnect in emergency situations despite loss of view and loss of control conditions in the SCADA environment. Given the inability to verify protection logic, field personnel tasked with restoration would likely reconnect opened breakers on transmission lines absent relay protection. Depending on circumstances, consequences could range from immediate system damage due to overcurrent conditions to delayed impacts from a future fault condition taking place before the hazardous condition is discovered and remediated. While precise predictions of what would occur are difficult to impossible given the potential for backup or non-digital protection equipment on site, attack intentions based on deployed capabilities appear quite clear: to take advantage of operational responses to create hazardous conditions at the transmission site, yielding potential physical equipment damage. Had such an attack been successful, the outage would have increased from hours to possibly weeks or months as damaged transmission gear was replaced.

[37] What is a Protection Relay – Littelfuse; The Art & Science of Protective Relaying – C. Russell Mason, GE
[38] Advisory ICSA-15-202-01 Siemens SIPROTEC Denial-of-Service Vulnerability – US-CERT
[39] Advisory ICSA-15-202-01 Siemens SIPROTEC Denial-of-Service Vulnerability – US-CERT
[39] Picture of Siemens SIPROTEC device post-DoS attack, from the lab of Reid Wightman.

One additional theory concerning CRASHOVERRIDE's involvement with protective relay technology is that the event was a precursor to or setting up for an Aurora-like event. The Aurora generator test, covered more extensively below, relies on manipulating protection systems to close out of synchronization with overall grid activity. The intention is to increase physical system stress to the point of causing damage to connected rotating equipment (e.g., generators).[40] Some have speculated that CRASHOVERRIDE encompasses an Aurora-like effect,[41] yet all existing evidence of tool capability and adversary actions indicates this is not only unsupported by event details, but outside the scope of attack capabilities. Given focus on transmission systems and no capability to manipulate relays beyond the denial of service condition, drawing comparison to an Aurora-like effect is not merely unsupported but fundamentally irrelevant. Discussion of actual Aurora risks will be presented later in this paper.



Create Large-Scale Transmission Outage
Wiper Event Produces Loss of View, Loss of Control
DoS SIPROTEC Protective Relays
Anticipate Rush to Physical Restoration
• Timing coincides with 2015 event
• Pressures utitility to restore ASAP
• Wiper delays restoration
• More importantly degrades visibility into SCADA
• Remove transmission protection on de-energized line
• Loss of view makes this difficult to ascertain
• Create conditions for overcurrent event
• SIPROTEC DoS results in physical damage

Figure 2: Revised CRASHOVERRIDE Attack Flow

While CRASHOVERRIDE ultimately failed to work as intended for various reasons – from improperly designed ICS communication to an apparent software development error rendering the SIPROTEC DoS inert – the attack as designed represents a dramatic increase in ambition, planning, and attempted execution. Successful execution required proper sequencing and understanding of operator responses, but if achieved could have produced a greater outage time, due to equipment damage or destruction rather than the relatively trivial impact actually observed. Two critical elements make this transition from short-term disruption to potential long-term disruption possible: first, the ability to severely degrade process visibility and control following the outage; second, being able to remove line protection at transmission sites to enable a hazardous condition to exist. When combined with the intended scale of the outage, CRASHOVERRIDE evolves into

[40] Mitigating the Aurora Vulnerability with Existing Technology – Dough Salmon, Mark Zeller, Armando Guzman, Venkat Mynam, and Marcus Donolo, Schweitzer Engineering Laboratories
[41] OT Networking Personnel need to Work with Engineering to Address Safety Impacts – It isn't Happening – Joe Weiss

a complex, multi-stage attack displaying significant (if imperfect) knowledge of electric transmission operations to produce a much more serious impact than the 2015 event.

The exact implications and efficacy of the attack had it been properly implemented and executed remain a matter of conjecture. While the overall hazardous condition of the transmission substation following successful execution would be deeply concerning, the presence or availability of physical protection systems and backup equipment may have mitigated against a worst-case scenario effect. Irrespective of these systems and their potential efficacy, a thorough analysis of CRASHOVERRIDE's execution and sequencing reveals worrying ambitions to undermine process integrity and protection even if the actual results in this specific instance may never be known.

TRISIS/TRITON

TRISIS, also known as Triton, first emerged publicly in December 2017 as a safety system-focused event occurring in Saudi Arabia.[42] Subsequent public reporting identified the victim as an oil and gas refinery,[43] but also indicated that there were multiple, distinct events instead of a single discrete outage. Specifically, safety systems within the plant were tripped not only in August 2017 (prompting the investigation eventually identifying TRISIS malware), but two months prior in June 2017 as well.[44]

Similar to CRASHOVERRIDE's deployment, TRISIS execution was the final step in a long-term, multi-stage intrusion into the victim environment to achieve proper access and attain relevant information to enable an ICS attack.[45] While much subsequent reporting on TRISIS focused on the plant disruption created when the targeted safety instrumented system (SIS) faulted, this view mischaracterizes the event. First, an understanding of SIS functionality is necessary to understand TRISIS implications. As shown in Figure 3,[46] SIS serves as an automated safeguard between normal plant operations and physical controls and recovery in the event of unsafe conditions manifesting themselves in the plant environment. While physical protection systems will still exist within the plant, event migration beyond SIS mitigation results in far more concerning events and more difficult plant recovery.

Within the context of SIS functionality, TRISIS was not designed to directly disrupt the plant environment. TRISIS instead represents a directed effort to build an in-memory backdoor or rootkit-level functionality to allow an attacker to gain unfettered, undetected control over a Schneider Electric Triconex SIS. Of particular note, the attack is very narrowly tailored not just to Triconex equipment, but to older PowerPC-based Triconex

[42] TRISIS Malware – Dragos; Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure – Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, and Christopher Gloyer, FireEye
[43] The Inside Story of the World's Most Dangerous Malware – Blake Sobczak, E&E News
[44] Triton – A Report from the Trenches – Julian Gutmanis (S4 Conference); Trisis Investigator Says Saudi Plant Outage Could Have Been Prevented – Cyberscoop
[45] TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping – Steve Miller, Nathan Brubaker, Daniel Kapellmann Zafra, and Dan Caban, FireEye
[46] Basic Fundamentals of Safety Instrumented Systems, DVC6000 SIS Training Course – Emerson

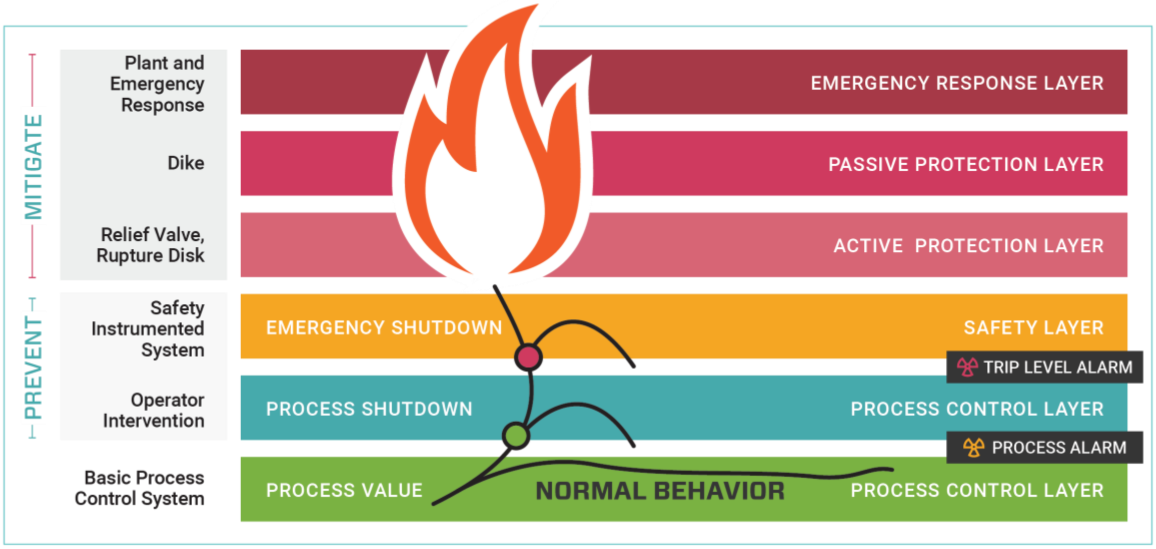


Figure 3: Diagram Showing SIS Functionality Relative to Other Systems[46]

versions running specific firmware revisions.[47] As a result, TRISIS is useful only within very limited circumstances – while the overall attack "playbook" of safety attacks is now publicly known, the ability to directly replay the specific malware for wider effects is extremely limited. Furthermore, the malware itself, unlike CRASHOVERRIDE, does not feature a built-in or automated manipulation functionality. Rather TRISIS provides the means for an adversary to alter the SIS undetected as part of an overall attack plan.

While TRISIS could be used by an attacker to directly trip or trigger the SIS to create a plant shutdown, this use case seems extremely unlikely. Given the investment in resources, development, and research to produce narrowly tailored malware designed for a specific version of the Schneider Electric Triconex SIS, a direct, disruptive event to shut the plant down could have been achieved through far simpler and cheaper means. That TRISIS tripped the Triconex devices within the victim environment thus appears to be a mistake and not a goal in itself. Instead, TRISIS sought a more elusive and far more malicious objective: to enable surreptitious access to the SIS devices while enabling arbitrary modification in SIS functionality after installation.

TRISIS was designed to take advantage of reserved network accessibility features in Triconex devices to establish a communication route to an in-memory implant – essentially a rootkit – enabling complete adversary control over the SIS.

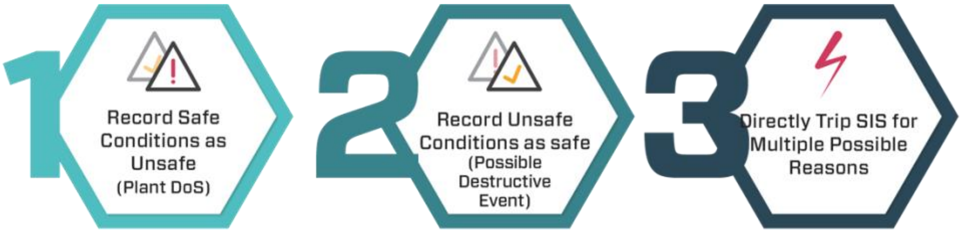

1
Record Safe Conditions as Unsafe (Plant DoS)
2
Record Unsafe Conditions as safe (Possible Destructive Event)
3
Directly Trip SIS for Multiple Possible Reasons

Figure 4: TRISIS Post-Installation Options

[47] MAR-17-352-01 HatMan – Safety System Targeted Malware – US-CERT

As such, this offers profoundly more complex and interesting functionality than simply disabling or disrupting the safety system. Given that the attacker was established on the engineering workstations connected to plant SIS equipment, the attacker could have directly manipulated or disabled devices producing something philosophically similar to the Ukraine 2015 event. By developing and deploying TRISIS, the attacker instead sought not to disable SIS functionality in the plant, but rather to enable arbitrary modifications to SIS operations.

An adversary capable of arbitrarily modifying SIS functionality undetected by plant operators opens several deeply concerning attack scenarios given compromise of plant safety and integrity, as illustrated by Figure 4. Perhaps most directly, an attacker could modify the SIS to identify normal operating parameters as unsafe, creating plant shutdowns during regular operations. Although costly and disruptive, such an attack route would be a waste of resources and access as an attacker capable of SIS modification could achieve this impact through other, less-costly means. More insidious and dangerous is modification of SIS parameters to inhibit or reduce SIS response to unsafe conditions, essentially removing safety controls from the process in a manner plant-operators would not be able to observe or identify.

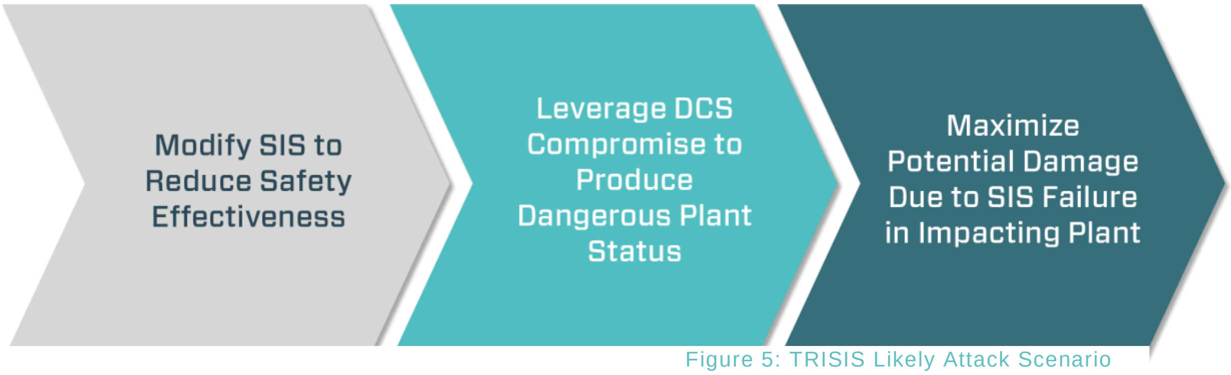

Modify SIS to Reduce Safety Effectiveness
Leverage DCS Compromise to Produce Dangerous Plant Status
Maximize Potential Damage Due to SIS Failure in Impacting Plant

Figure 5: TRISIS Likely Attack Scenario

Given the length of the intrusion leading up to TRISIS (based on publicly available discussion, potentially extending as far back as 2014)[48] and breadth of victim compromise across both IT and ICS networks, the attacker (referred to as XENOTIME by Dragos)[49] would be able to execute some very interesting attack scenarios. Although we cannot immediately confirm this, based on public reporting on the extent of victim compromise it is very likely that the attacker had access to the plant distributed control system (DCS) environment as well as the safety environment. Pairing these compromises yields possibilities for significant control over plant operations and safety response. For example, rather than simply modify the SIS via TRISIS and wait for an unsafe condition to appear "naturally," the attacker could modify multiple Triconex

[48] Triton – A Report from the Trenches – Julian Gutmanis (S4 Conference)
[49] XENOTIME - Dragos

devices and then alter the DCS to produce a specific type of process upset condition – one tailored to the modifications made in plant safety. In this respect, the attacker could engineer a dangerous (and potentially deadly) event in the plant environment through a multi-stage intrusion and modification of plant safety and integrity.

The combination of likely DCS compromise with arbitrary control over plant safety mechanisms thus produces considerably worrisome and ambitious attack scenarios. While public reporting identifies TRISIS as “malware that can kill,”[50] TRISIS itself represents one component in a series of staged, sequenced events to bring about such a concerning state. Instead, it is more accurate to say that TRISIS is a necessary, intermediate step in a complex infection and modification sequence to undermine plant safety producing hazardous conditions that would be favorable for manufacturing catastrophic process events. Some may argue the above is so much semantics, but drawing such distinctions is critically important for understanding what TRISIS means for ICS environment safety and how it fits in to overall attack logic.

Essentially, TRISIS was designed as a very specific tool to undermine the integrity of plant safety by enabling arbitrary access to and modification of plant SIS. As such, it represents just one piece (albeit a critical one) in an overall sequence of events required to yield actual destruction. Post-modification, an attacker can either wait for an unsafe event to materialize organically within the environment, or leverage access to DCS to produce unsafe conditions at a time of their choosing. In either case, the fundamental integrity of process safety is degraded, leaving the plant (and workers therein) exposed to potentially catastrophic, hazardous conditions.

Based on what was observed in the victim environment and subsequent public reporting, TRISIS as designed and as intended in the most-likely attack scenarios failed. When TRISIS caused the victim SIS to trip on installation, it interrupted the attack flow by causing an undesired disruption in the plant environment. Similar to CRASHOVERRIDE, TRISIS represents a worrying escalation in attacker capabilities and ambitions with respect to eroding ICS integrity en route to likely physical destruction – but based on all available evidence, TRISIS’s ambitions were never truly realized.

Evaluating Attack Efficacy and ICS Resilience

After the above overview, we are left with an interesting observation: of three cyber-oriented, integrity-based attacks, only one (Stuxnet) appeared to succeed in its intended function. Even then, one could argue that Stuxnet’s impact was somewhat less than intended given that the malware appears to have been caught earlier than anticipated by its developers.[51] The “success rate” of ICS events may therefore cause some to question the efficacy and seriousness of cyber-nexus ICS attack scenarios – yet such an approach would be deeply misguided by ignoring the totality of adversary activity, if

[50] TRISIS/TRITON and the Rise of Malware Built to Kill – The Cyberwire
[51] Obama Order Sped Up Wave of Cyberattacks Against Iran – David Sanger, The New York Times

not criminally negligent for overlooking the potentially catastrophic consequences of events to date had one or more elements operated as intended.

While Stuxnet represents somewhat of an outlier in terms of functionality and success, the overall trendline of events including CRASHOVERRIDE and TRISIS clearly indicate that adversaries possess the intent and desire to build complex cyber-nexus ICS attack scenarios leading to potential physical damage. Post-Stuxnet events have largely failed due to immature attacker understanding of ICS environments and unforeseen consequences when deploying capabilities “in the wild”. Yet the broader pattern of pre-attack activity observed in the ICS space – such as extensive, alleged Russian probing of the US, UK, and other electric sectors[52] - indicates sustained commitment to gain access to and learn about ICS environments, typically associated with geo-political tensions.

ICS attackers remain committed to developing and attempting complex ICS attack scenarios. While attacks to date have not achieved the level of success desired given likely intent and attack design, such errors are due to oversight on the part of the attacker as opposed to any direct or conscious action on the part of ICS asset owners or network defenders. More concerningly, adversaries are learning and improving over time, most vividly demonstrated in the attack evolution from 2015 to 2016 in Ukraine.

The requirements and technical complexity involved in designing, delivering, and executing an integrity-focused ICS attack remain significant – but such barriers are not insurmountable. Given continued adversary pursuit of such effects, ICS asset owners and defenders should anticipate future efforts to execute this type of complex, multi-stage attack sequence. While examples to date provide few samples of successful attacks around which defenders can plan and prepare, possible attack scenarios are not difficult to think of, even if they thankfully remain difficult to execute and master.

Future Attack Scenarios

Given the above events and expectations that potential ICS attackers are not going away, ICS asset owners and defenders must concern themselves not only with past attack scenarios but future possibilities as well. Unfortunately, the overall scope and potential attack surface for ICS attacks is vast, providing adversaries with a number of options not just for direct process disruption but for integrity-based attacks as discussed previously.

The following sections will outline potential scenarios either within reach of adversaries today, or not far off in attacker capability development. While the following ideas are within the realm of the possible, it is also important to note that many (if not most) are relegated to the land of the improbable. That is, while a sufficiently skilled, well-

[52] Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors – US-CERT; America’s Electric Grid Has a Vulnerable Back Door – And Russia Walked Through It – Rebecca Smith and Rob Barry, The Wall Street Journal

resourced, motivated, and perhaps most importantly patient adversary may be able to achieve any of the subsequent attack scenarios, the likelihood of doing so (successfully) is relatively low at present.

Nonetheless, even though attack success probability currently appears small, potential attack impact remains very high. As a result, asset owners must still recognize and where appropriate prepare for such scenarios to ensure adequate defense and overall operational resiliency.

ELECTRIC UTILITY DISRUPTIONS

Electric sector attacks in ICS often receive the most public and media attention, as well as extensive public and private analysis due to this sector's importance in enabling all other critical infrastructure verticals.[53] In some cases, security firm private telemetry even indicates the electric sector faces the most attacks of any ICS-related industry.[54] However, the primary focus of such past analysis has been on direct disruption or destruction, where an infection or intrusion event results in immediate impacts on one element of electric sector operations (generation, transmission, or distribution). Multi-stage attack scenarios targeting electric sector process integrity are either seldomly explored or ignored outright, yet possibilities exist for electric sector impacts through similar methodologies as CRASHOVERRIDE.

Protective relay attacks have already been addressed to some extent in the CRASHOVERRIDE example, but the possibilities for digital protective relay manipulation or modification extend beyond the 2016 Ukraine scenario. Relay protection works for safeguarding both transmission and generating assets. An attack such as the CRASHOVERRIDE scenario could be modified to remove or modify line protection in such a fashion to weaken fault protection to either steadily degrade physical assets over time (i.e., by modifying time tolerances to increase equipment stress) or enable direct asset loss by preventing fault protection during a specific incident (either triggered by an attacker or waiting for a "natural" event). In either case, the goal becomes similar to what was likely attempted in CRASHOVERRIDE: producing physical destruction of transmission equipment, especially substation transformer equipment.

The above scenario becomes concerning quickly, given the small (or nonexistent) supply of backup equipment for critical transmission and long lead times for producing new equipment.[55] By gaining sufficient access to a handful of critical transmission sites without being detected, an attacker could undermine protective relay logic to enable physical damage to transmission equipment at multiple locations nearly simultaneously. The resulting shift in electric transmission to ever-fewer pathways can create increased stress on underlying electric infrastructure, enabling the potential for possible wide-spread impacts as grid components begin to self-protect causing continual ripple effects.

[53] Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector – Idaho National Laboratory, US Department of Energy
[54] Threat Landscape for Industrial Automation Systems in H2 2017 – Kaspersky Lab
[55] Transformers Expose Limits in Securing Power Grid – Rebecca Smit, The Wall Street Journal

Examples such as the 2003 US and EU blackout events – where a combination of limited backup capacity, poor maintenance, and cascading self-protection events produced widespread loss of electricity[56] – now become possible with an initial cyber impetus. Of note in this scenario, the actual outage is merely facilitated by attackers undermining protection systems within critical infrastructure, with the resulting lack of process integrity causing disruption.

For generation, similar principles with different impacts apply. One of the earliest and most alarming attack vector disclosures for electric generation came with discovery of the Aurora generator test in 2007.[57] The Aurora attack seeks to "intentionally open a breaker and close it out of synchronism to cause damage to connected power system equipment, such as generators, motors, and transformers."[58] When the breaker is closed out of sync, the impacted generator will experience significant torque and physical strain while trying to re-synch with the overall electric grid. Done multiple times in a short interval, such an attack can cause a rotating asset to destroy itself. Numerous safeguards exist to prevent or mitigate such an attack, but subtle integrity attacks – especially on protective relays for generating sites – enable means to execute an Aurora event in a difficult-to-detect manner. Although such an attack would be extremely difficult to properly execute given the combination of logical and physical safeguards and other mitigating factors, events such as TRISIS and CRASHOVERRIDE indicate adversaries are willing to attempt complex, multi-stage attack vectors, so this cannot be ignored.

While direct communication to breakers to open and close them (similar to breaker manipulation used in transmission operations in CRASHOVERRIDE) can immediately create circumstances for an Aurora-like effect, this attack vector has multiple problems rendering it likely immaterial if not outright irrelevant. First, direct manipulation of breakers and related equipment introduces noticeable lag in responsiveness between attacker-initiated action and physical response of actual breaker equipment. Thus, direct manipulation of equipment to achieve an Aurora-like impact is either extremely difficult, or outright impossible. Furthermore, such communication can (hopefully) be detected during execution or in staging steps prior to launch. Instead of the above scenarios (or something similar to CRASHOVERRIDE where protection logic is simply removed), a much more effective (if difficult) attack vector lies in modifying breaker logic or functionality to create subtle changes in behavior that weakens protection. As stated previously, such impacts would include modifying tolerances for automated responses. Such an alteration to protective relay functionality – whether through direct modification of relay logic or through a TRISIS-like exploitation of relay software to enable unmonitored, arbitrary access to relay functionality – would be far more difficult to

[56] Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations – US-Canada Power System Outage Task Force; Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy – UCTE

[57] Mouse Click Could Plunge City into Darkness, Experts Say – CNN

[58] Common Questions and Answers Addressing the Aurora Vulnerability – Mark Zeller, Schweitzer Engineering Laboratories

diagnose, while either enabling direct impacts or creating circumstances causing damage over time.[59]

All of the above scenarios can be executed in a semi-direct, staged fashion where incidents follow each other in sequence to produce the intended physical effect, as was likely the intention in CRASHOVERRIDE. However, integrity-based attacks provide some interesting scenarios for adversaries who are either patient or opportunistic, by taking advantage of natural grid events to serve as the catalyst for bringing about physical impacts via modified process integrity. Nearly all examples of large-scale blackout events in modern electric utility systems depend upon multiple failures impacting stressed infrastructure (e.g., high demand periods, or significant equipment removed from operations for maintenance reducing "slack"). Modern protection systems, balancing authorities, and other safeguards exist within the context of a "N-1" reliability standard – ensuring that the loss of any single asset does not result in systemwide shutdown.[60] In high-stress conditions where exogenous factors already limit grid resiliency, an attacker can deliver an impact at this critical point in time to "nudge" the overall electric system into crisis.[61]

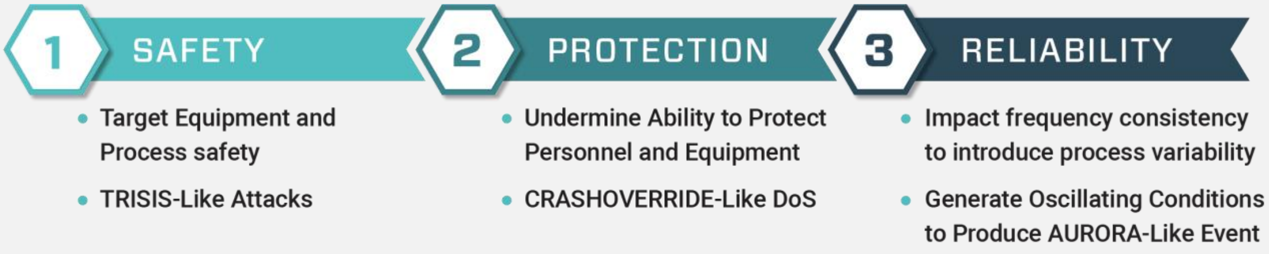

1
SAFETY
Target Equipment and Process safety
TRISIS-Like Attacks
2
PROTECTION
Undermine Ability to Protect Personnel and Equipment
CRASHOVERRIDE-Like DoS
3
RELIABILITY
Impact frequency consistency to introduce process variability
Generate Oscillating Conditions to Produce AURORA-Like Event

Figure 6: Electric Sector Integrity Attack Options

Examples of the above include waiting for periods of high demand with little or no spare capacity such that "N-1" reliability no longer satisfies reliability needs – a scenario frequently observed in deregulated energy markets such as the ERCOT[62] service area. Trends in variable generating resources – particularly renewables – produce built-in system stress periods as defined by the "duck curve" showing time-period imbalances between demand and generation.[63] Such circumstances can serve as either the trigger for a latent integrity modification to manifest as widespread disruption, or for a direct disruptive event to metastasize as a far larger crisis. Understanding interconnections between dependent entities in overall electric utility operation – and the potential

[59] Myth or Reality – Does the Aurora Vulnerability Pose a Risk to My Generator? – Mark Zeller, Schweitzer Engineering Laboratories
[60] Electric Transmission Reliability Management – Marten Ovaere, IAEE Energy Forum; Reliability Concepts – North American Electric Reliability Corporation (NERC)
[61] Kicked While Down: Critical Infrastructure Amplification and Messaging Attacks – Joe Slowik
[62] Summer Price Spikes are a Feature of Texas' Power Market, Not a Bug – Joshua Rhodes, Axios
[63] Confronting the Duck Curve: How to Address Over-Generation of Solar Energy – US Department of Energy

consequences of a modification to any one element in the system to all other parties within the grid – is vital to planning for and responding to such potential events.

MANUFACTURING ATTACKS

Stuxnet fundamentally represents an attack on manufacturing, in such a way that overall process reliability and confidence were attacked to impair operations. Research surrounding potential ICS attacks on manufacturing environments – such as the manipulation of industrial robots[64] or the increasing presence of self-propagating malware in facility networks[65] – has increased significantly in the past five years. Yet fundamental attacks on process integrity in manufacturing operations, given complexity and expense, would appear to be limited to strategically-significant targets rather than more general targeting of manufacturing entities. Thus, we can look at integrity-focused manufacturing attacks as likely impacting critical sectors such as the defense industrial base[66] or related sectors tied to national security.

Along these lines, manufacturing attacks can focus on two primary integrity aspects: overall process reliability (as was the case in Stuxnet) or impacting production outputs to increase failure or defect rates. While no confirmed, publicly-known instances of the latter exists at present, multiple outlets have reported on potential US intrusions into North Korea's ballistic missile program to sabotage designs and production.[67] Such supply chain-focused attacks are hardly new – and may have played a role in the overall Olympic Games program which included Stuxnet.[68] Hints and rumors of similar activity abound in stories of clandestine activity. Examples range from alleged (and disputed) CIA tampering of oil and gas supply chain parts during the Cold War[69] to more recent rumors of US sabotage of Iran's ballistic missile program.[70] Overall, critical or defense manufacturing sabotage (including through cyber means) has been and remains a tactic used by intelligence entities for clandestine disruptive activity.

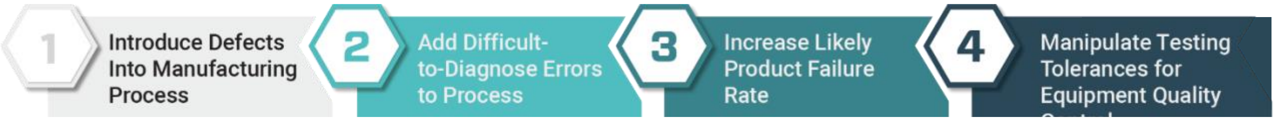

1
Introduce Defects Into Manufacturing Process
2
Add Difficult-to-Diagnose Errors to Process
3
Increase Likely Product Failure Rate
4
Manipulate Testing Tolerances for Equipment Quality

Figure 7: Manufacturing Integrity Attack Options

[64] Rogue Robots: Testing the Limits of an Industrial Robot's Security – Federico Maggi, Davide Quarta, Marcello Pogliani, Andrea M. Zanchettin, and Stefano Zanero, TrendMicro
[65] NotPetya Ransomware Outbreak Cost Merck more than $300M per Quarter – Conner Forrest, TechRepublic
[66] Defense Industrial Base – US Department of Homeland Security
[67] Hand of U.S. Leaves North Korea's Missile Program Shaken – David E. Sanger and William J. Broad, The New York Times; Trump Inherits a Secret Cyberwar Against North Korean Missiles – David E. Sanger and William J. Broad, The New York Times; Trump Hints that the US May be Sabotaging North Korea's Nuclear Program – Alex Lockie, Business Insider
[68] The Sabotaging of Iran – Roula Khalaf, James Blitz, Daniel Dombey, Tobias Buck, and Najmeh Bozorgmehr, The Financial Times
[69] CIA Plot led to Huge Blast in Siberian Gas Pipeline – Alec Russell, The Telegraph; Soviets Burned by CIA Hackers? – Wired
[70] U.S. Revives Secret Program to Sabotage Iranian Missiles and Rockets – David E. Sanger and William J. Broad, The New York Times

Modification of manufacturing logic at the production level for malicious purposes has been demonstrated within the realm of 3D printing,[71] and remains a persistent concern in high-visibility, high-expense defense projects such as the F-35 airplane program.[72] As shown in Figure 7 above, the range of possibilities range from straightforward manipulation of manufacturing processes to multi-stage events seeking to alter not just manufacturing processes (to increase defects or failure rates) but also to harm testing or quality assurance mechanisms to hide such manipulations at the point of post-production analysis.

The level of effort required (and lack of monetary motivations behind such attacks) mitigates against such attacks becoming widespread throughout manufacturing verticals. But organizations involved in critical defense industries, or potentially high-impact areas such as pharmaceuticals, must be wary of such an attack vector and its implications. Through difficult to execute (as shown in the example of Stuxnet), such attacks are not impossible – and when successful are extremely difficult to diagnose and effectively remediate.

OIL & GAS INTRUSIONS

Oil and gas sector attacks incorporate multiple potential vectors for integrity-specific impacts ranging from product quality manipulation through cyber-physical effects endangering safety or causing physical destruction. As previously explained by Dragos, the overall oil and gas threat environment is becoming more active and hostile, with multiple entities attempting to develop capabilities for or gain footholds within this industry.[73] While only one known event has actively sought to compromise operational integrity (specifically safety) in an oil and gas environment (TRISIS), the scope for potential attacks is large.

The most obvious and concerning attack vector mirrors the TRISIS scenario, where attackers compromise plant safety or alter SIS equipment while engineering a disruptive scenario to cause physical damage. Previous discussions of such attack paths have focused on either application-layer attacks (e.g., compromising a device via vulnerability to gain access and directly modify it) or inadvertent change concerns as being most-likely scenarios in this realm.[74] However, the TRISIS event shows attackers are able to develop far more subtle attacks moving beyond direct manipulation of control to modifications that are potentially invisible to plant operators. By impacting integrity under a fundamental loss of view scenario, attackers can either leverage known responses to plant operations to facilitate an attack (a scenario similar to CRASHOVERRIDE) or utilize

[71] Successful Sabotage of Drone Highlights Additive Manufacturing Security Needs – Karen Haywood Queen, Advanced Manufacturing
[72] Pentagon is Rethinking its Multibillion-Dollar Relationship with U.S. Defense Contractors to Boost Supply Chain Security – Ellen Nakashima
[73] Dragos Oil and Gas Threat Perspective Summary – Dragos
[74] ICS Cybersecurity: You Cannot Secure what you Cannot See – David Zahn, PAS

additional access to produce unsafe conditions which will not be caught by automated systems.

Fundamental to safety and protection attacks within the oil and gas space are multi-stage attacks working to undermine integrity at the safety and protection level while leveraging more widespread process control network (PCN) access to control or initiate dangerous plant conditions. By pairing these two parallel intrusions, attackers gain complete control over plant operations and automated safety responses. Such access can then be used to build up or trigger complex attacks resulting in significant physical damage.

Outside of oil and gas production operations, interesting attack scenarios can also play out for midstream operations, specifically pipelines in the natural gas transportation sector. Gas transportation already features significant risks in the event of mechanical failures concerning over pressurization and related conditions, shown dramatically in several recent accidents in the United States.[75] While some events (most notably the 2018 series of events resulting in multiple explosions in Massachusetts[76] and the 2008 Turkish pipeline explosion[77]) were initially greeted with fears of potential cyber operations, subsequent investigation and reporting identified far more mundane (if still very serious) causes.

Yet the scope for pipeline equipment compromise and manipulation is significant, even if no such known attacks have occurred to date. Recently, cyber intrusions into natural gas operations appear to have increased in frequency, such as the 2018 intrusion into electronic data interchanges used by natural gas pipelines.[78] While no such operations have yet gained access to actual control systems, adversaries appear determined to gain greater access to these networks. Such access could be used to facilitate subsequent disruptive events, including manipulation of compressor stations or sensor telemetry to either cause or enable potentially dangerous and destructive scenarios.

Defense and Response

The above scenarios present concerning and potentially dangerous problems for ICS asset owners and operators. More concerning still, the nature of these attack vectors mean that they extend well beyond traditional, IT-centric network defense by incorporating various ICS-specific elements of operations. Given this unique combination of multiple factors – from IT-based intrusions to process-specific manipulations to physical consequences – single-source identification and alerting is insufficient for

[75] Federal Investigators Pinpoint what Caused String of Gas Explosions in Mass. – Merrit Kennedy, NPR; Enbridge Needs U.S. Approval to Restart Natgas Pipe after Kentucky Blast – Reuters
[76] Safety Recommendation Report – Natural Gas Distribution System Project Development and Review (Urgent) – US National Transportation Safety Board
[77] Türkische Pipeline-Explosion wohl kein Cyber-Angriff – Hakan Tanriverdi, Suddeutsche Zeitung; Closing the Case on the Reported 2008 Russian Cyber Attack on the BTC Pipeline – Rob M. Lee, SANS
[78] Attack on Natural Gas Network Shows Rising Cyberthreat – Blake Sobczak, E&E News

defensive monitoring and response. Furthermore, adequate analysis to ensure restoration of known-good, known-safe processes occurs demands abilities in forensic and process analysis well beyond typical methodologies (or asset owner capabilities and resources) at present.

While some voices might posit that circumstances demand defense and monitoring down to the level of individual sensor inputs within a process environment to ensure continued integrity and viable defense, the overall threat environment to date does not support such an exaggerated response. Although future scenarios may incorporate such fundamental, layer 0-type impacts, at present adversaries have all the required capability necessary to cause damage while working largely in a Windows-based environment with some understanding of control system logic and process interconnection. Based on what is actually occurring in real-world scenarios, asset owners and operators must focus attention on the problems of today and the near future, which thankfully can be solved through better analysis and use of existing data while fusing IT security knowledge with ICS process expertise.

PROCESS-CENTRIC AWARENESS AND MONITORING

First and foremost, in ICS environments the fundamental combination of IT technologies with physics means that an IT-specific monitoring and analysis perspective will miss important details in incident analysis and response. Rather than focusing on network observables alone, ICS-oriented detection, response, and remediation must take into consideration process-specific data to identify those instances where IT-centric actions or changes may propagate (or have already done so) to actual physical processes.

Industrial environments are already awash in data from physical processes – from device information to process telemetry. Yet although such extensive data exists (and is recorded), little analysis and evaluation is performed on such a rich dataset. But the fundamental impacts and influences of ICS attacks – especially those seeking to subtly undermine fundamental process integrity – will necessarily manifest themselves in process-centric data. Failing to incorporate process communication and traffic monitoring as part of an overall security response posture thus leaves significant space available to potential attackers to execute their mission within control system environments.

Thus, the first and foremost recommendation for industrial entities with respect to ICS-specific security is to take advantage of information sources already available: process monitoring[79] and telemetry traditionally captured by historians or related products for

[79] Of note, "process monitoring" refers to the existing ingest and analysis of process operations for long-term operational awareness and health monitoring. While multiple commercial solutions exist at the time of this writing proposing "out of band", dedicated sensors to monitor for process-centric anomalies, such devices either ignore or are unaware of the fundamental concerns documented by this paper – of identifying alterations to process logic in an undesirable (but allowed) fashion to create potentially hazardous conditions. Such an attack vector requires identifying not just that something has been altered on the process level, but

overall environmental awareness or specific functionality. Given this visibility, asset owners, operators, and defenders can then identify those exceptional circumstances (such as CRASHOVERRIDE or TRISIS) where adversaries have fundamentally altered the operational environment in such a manner as to make cyber-physical impacts not only likely, but very real and dangerous. Absent such visibility, asset owners are left in the dark with ambiguous IT-centric identifications and alerts that may identify precursors to ICS-specific attacks, but provide little or no information as to the extent of such impacts – and how they may influence response and recovery efforts.

An outlier scenario exists where process data is manipulated, spoofed, or altered as part of an attack scenario, as observed in portions of the Stuxnet event. In these cases, combining data sources (as well as incorporating basic operator observations of the environment even when in conflict with data) is necessary to ferret out potentially dangerous scenarios. At present, all known adversary capability at this level exists at the software alteration or traffic spoofing level, rather than fundamental manipulation of telemetry sources. Given this type of integrity attack, process-aware network security monitoring combined with plant observations can begin to identify those anomalous conditions of spoofing or traffic replay to hide malicious activity.

EVENT CORRELATION

While IT-centric information is insufficient on its own to detect and respond to ICS-relevant events, it still forms a significant (and necessary) part of the overall defense and monitoring process. The increasing digitization of ICS environments – the “IT-OT convergence” – means that IT-based systems (and their security problems) are proliferating within industrial environments. While working to expand attack surface and facilitate attacker movement, such developments also make available a host of potential data, collection points, and defensive operations that, when taken advantage of in light of industrial process fundamentals, allow for more robust system monitoring.

For multiple reasons – such as device applicability, process understanding, and response limitations – IT-centric solutions on their own will not suffice for ICS defense, but when used in concert with process-centric observations powerful options become available. Looking at all three events covered in detail in this paper, opportunities existed where otherwise “low signal” or “merely anomalous” observations in either IT or ICS environments could be combined and correlated to indicate a concerning event was in progress. For example, in CRASHOVERRIDE, the combination of malware execution, operational loss, and isolated communication to protective relays could be fused to indicate a more complex scenario unfolding than just the immediate outage event. Similarly, accurate recording and analysis of events during the TRISIS incidents could have married network detection data (or even information as basic as network flow) to identify communication to safety workstations in the immediate period before SIS

being able to orient and identify such a change in light of broader network activity to enable root cause analysis and a restoration of process integrity.

malfunction to narrow investigation to potential malicious or unauthorized access to safety resources.

Plant operators must work to gather, add appropriate context to, and then fuse available information from events from all available sources to build out accurate, near real-time pictures of environment operations. This goes well beyond the anomaly detection idea of just flagging “unusual” or “odd” but moves operators into positions to act on enriched, meaningful events based on the combination and correlation of multiple sources in time-series fashion. Complex, difficult-to-detect (in isolation) intrusions and manipulations require detection methodologies rooted in adversary behavior that can appropriately combine sources to yield high-confidence detections of malicious activity.[80] Through this threat behavior-based approach, asset operators can ensure greater visibility into the plant security environment to detect integrity-focused attacks as they unfold.

ENABLING RECOVERY AND RESTORATION

Finally, organizations must be appropriately prepared and capable to respond to ICS attacks, including those attacks which impact fundamental industrial operation characteristics. Many of the scenarios that either have already taken place or outlined as possibilities in this paper focus on the critical elements of process protection and process safety. When responding to events that may impact these vital characteristics of industrial operations, ICS asset owners and operators must exercise great care in investigating and restoring operations to ensure the impacted process is brought up in a known good, verified safe state.

First, even determining that an integrity modification or integrity-based attack has occurred is problematic given the likely focus of such attacks on non-standard, vendor- and application-specific systems. The ability to perform sound forensic analysis may be difficult to impossible due to operating systems or other aspects of the targeted equipment. Even relatively simple steps such as performing a “diff” of configuration data may not be possible if configuration data is not stored offline and updated with every change in the process environment. Asset owners need to identify these detection and analysis gaps in advance, as solving such problems in the middle of a potential incident – especially one resulting in process shut-down – only increases the likelihood of mistakes or oversight.

Second, operational restoration must take into consideration not just restoring impacted or infected IT-like systems, but performing adequate checks to determine if such access was leveraged to perform other modifications within the environment. Similar to the first recommendation, being able to answer these questions is critical, but even ensuring they are asked (especially in a “rush to restore” situation) is vital. Operational and restoration checklists, standard operating procedures, and similar administrative controls can be

[80] The Four Types of Threat Detection with Case-Studies in Industrial Control Systems (ICS) – Sergio Caltagirone and Robert M. Lee, Dragos; Indicators vs. Anomalies vs. Behaviors: A Critical Examination for ICS Defense – Joe Slowik (CS3STHLM Conference)

applied to ensure that these questions are considered when restoring a disrupted process.

Finally, in many cases the knowledge required to adequately analyze potentially modified equipment (such as a Schneider Electric Triconex) resides in only a handful of places: the equipment vendor and certain specialty contractors. When faced with situations well beyond the experience or expectations of everyday plant and security personnel, asset owners should identify appropriate points of contact in advance for assistance in investigation. Working on this step after an incident occurs wastes time and further delays recovery, while also risking the potential loss of valuable information and artifacts to facilitate post-incident investigation.

Conclusion

ICS-targeting adversaries are growing increasingly aware of and willing to target fundamental operational principles of industrial processes to either maximize damage, inhibit recovery, or evade identification. The progression of events from Stuxnet to the present indicates continued adversary willingness to learn about industrial environments, what critical processes and equipment are necessary to maintain fundamental industrial process integrity, and how to undermine or remove that integrity for malicious purposes. While these attacks are complex and difficult to execute, resulting in multiple adversary failures in execution, all available evidence indicates attackers continue to work on developing and deploying such attack types given their outsized impacts.

Given this increasingly hostile environment, ICS asset owners and operators must adapt to and co-evolve with adversary tradecraft to ensure plant security and safety. Understanding that attackers are no longer simply seeking to turn a process off, but rather are aiming for ways to produce dangerous or hazardous situations, is a first and critical step. Subsequent activity must adapt existing visibility into industrial networks and processes to identify such attacks when they occur, and identifying gaps to address in advance of potential malicious activity. Through a commitment to continued defensive evolution guided by an understanding of the threat landscape, ICS asset owners can meet the challenges posed by integrity-based ICS attacks to preserve process accuracy, protection, and safety against determined attackers.

Works Cited

ALLANITE – Dragos

DYMALLOY – Dragos

Dragonfly: Cyberespionage Attacks against Energy Suppliers – Symantec

Implications of IT Ransomware for ICS Environments – Joe Slowik, Dragos

Win32.Stuxnet Dossier – Nicolas Falliere, Liam O Murchu, and Eric Chien, Symantec

Analysis of the Cyber Attack on the Ukraine Power Grid – Robert M. Lee, Tim Conway, Mike Assante (SANS Institute and E-ISAC)

Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE – Joe Slowik, Dragos (Virusbulletin 2018)

TRISIS Malware – Dragos

The CIA Triad – The Infosec Institute

Win32/Industroyer – A New Threat for Industrial Control Systems – Anton Cherpanov, ESET

Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure – Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, and Christopher Gloyer, FireEye

NSA/CSS Technical Cyber Threat Framework v2 – National Security Agency/Central Security Service

US Department of Defense Joint Publication 3-13 – Information Operations – US Joint Chiefs of Staff

'Operational Preparation of the Environment': 'Intelligence Activity' or 'Covert Action' by Any Other Name? – Joshua Kuyers

Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group – Symantec

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors – US-CERT

Electric Sector Targeting in Context – Joe Slowik

ISA-62443-2-1-2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program – International Society of Automation

Incident Response for Industrial Control Systems – Chris Sistrunk, FireEye

Defending ICS Networks against Cyber Attacks with Better Log Correlation – Harry Thomas, Forescout

What is ICS Security? – Chris Brook, DigitalGuardian

SCADA Security Basics: Integrity Trumps Availability – Eric Byres, Tofino Security

German Steel Mill Cyber Attack – Robert M. Lee, Michael J. Assante, and Tim Conway, SANS Institute

How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History – Kim Zetter, Wired

Stuxnet Logbook, Sep 16 2010, 1200 Hours MESZ – Langner Group

Stuxnet: Targeting Iranian Enrichment Centrifuges in Natanz? – Frank Rieger, Knowledge Brings Fear

Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment – David Albright, Paul Brannan, and Christina Walrond, Institute for Science and International Security

To Kill a Centrifuge – Ralph Langner, Langner Group

Uranium Enrichment – United States Nuclear Regulatory Commission

Obama Order Sped Up Wave of Cyberattacks Against Iran – David Sanger, The New York Times

Iran's Nuclear Program Suffering New Setbacks, Diplomats and Experts Say – Joby Warrick, The Washington Post

Iran Nuke Enrichment Sees Setback, Sources Say – George Jahn, Associated Press

Revealed: How a Secret Dutch Mole aided the U.S.-Israeli Stuxnet Cyberattack on Iran – Kim Zetter and Hulb Modderkolk, Yahoo News

Iran's Advanced Centrifuges – David Albright and Christina Walrond, Institute for Science and International Security

Performance of the IR-1 Centrifuge at Natanz – David Albright and Christina Walrond, Institute for Science and International Security

The Fordow Enrichment Plant, aka Al Ghadir: Iran's Nuclear Archive Reveals Site Originally Proposed to Produce Weapon-Grade Uranium for 1-2 Nuclear Weapons per Year – David Albright, Frank Pabian, and Andrea Stricker, Institute for Science and International Security

Iran's Long-Term Centrifuge Enrichment Plan: Providing Needed Transparency – Institute for Science and International Security

CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations – Dragos

Win32/Industroyer – A New Threat for Industrial Control Systems – Anton Cherpanov, ESET

CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack – Joe Slowik, Dragos

What is a Protection Relay – Littelfuse

The Art & Science of Protective Relaying – C. Russell Mason, GE

Advisory ICSA-15-202-01 Siemens SIPROTEC Denial-of-Service Vulnerability – US-CERT

Mitigating the Aurora Vulnerability with Existing Technology – Dough Salmon, Mark Zeller, Armando Guzman, Venkat Mynam, and Marcus Donolo, Schweitzer Engineering Laboratories

OT Networking Personnel need to Work with Engineering to Address Safety Impacts – It isn't Happening – Joe Weiss

The Inside Story of the World's Most Dangerous Malware – Blake Sobczak, E&E News

Triton – A Report from the Trenches – Julian Gutmanis (S4 Conference)

Trisis Investigator Says Saudi Plant Outage Could Have Been Prevented – Cyberscoop

TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping – Steve Miller, Nathan Brubaker, Daniel Kapellmann Zafra, and Dan Caban, FireEye

Basic Fundamentals of Safety Instrumented Systems, DVC6000 SIS Training Course – Emerson

MAR-17-352-01 HatMan – Safety System Targeted Malware – US-CERT

TRISIS/TRITON and the Rise of Malware Built to Kill – The Cyberwire

Obama Order Sped Up Wave of Cyberattacks Against Iran – David Sanger, The New York Times

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors – US-CERT

America's Electric Grid Has a Vulnerable Back Door – And Russia Walked Through It – Rebecca Smith and Rob Barry, The Wall Street Journal;

Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector – Idaho National Laboratory, US Department of Energy

Threat Landscape for Industrial Automation Systems in H2 2017 – Kaspersky Lab

Transformers Expose Limits in Securing Power Grid – Rebecca Smit, The Wall Street Journal

Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations – US-Canada Power System Outage Task Force

Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy – UCTE

Mouse Click Could Plunge City into Darkness, Experts Say – CNN

Common Questions and Answers Addressing the Aurora Vulnerability – Mark Zeller, Schweitzer Engineering Laboratories

Myth or Reality – Does the Aurora Vulnerability Pose a Risk to My Generator? – Mark Zeller, Schweitzer Engineering Laboratories

Electric Transmission Reliability Management – Marten Ovaere, IAEE Energy Forum

Reliability Concepts – North American Electric Reliability Corporation (NERC)

Kicked While Down: Critical Infrastructure Amplification and Messaging Attacks – Joe Slowik

Summer Price Spikes are a Feature of Texas' Power Market, Not a Bug – Joshua Rhodes, Axios

Confronting the Duck Curve: How to Address Over-Generation of Solar Energy – US Department of Energy

Rogue Robots: Testing the Limits of an Industrial Robot's Security – Federico Maggi, Davide Quarta, Marcello Pogliani, Andrea M. Zanchettin, and Stefano Zanero, TrendMicro

NotPetya Ransomware Outbreak Cost Merck more than $300M per Quarter – Conner Forrest, TechRepublic

Defense Industrial Base – US Department of Homeland Security

Hand of U.S. Leaves North Korea's Missile Program Shaken – David E. Sanger and William J. Broad, The New York Times

Trump Inherits a Secret Cyberwar Against North Korean Missiles – David E. Sanger and William J. Broad, The New York Times

Trump Hints that the US May be Sabotaging North Korea's Nuclear Program – Alex Lockie, Business Insider

The Sabotaging of Iran – Roula Khalaf, James Blitz, Daniel Dombey, Tobias Buck, and Najmeh Bozorgmehr, The Financial Times

CIA Plot led to Huge Blast in Siberian Gas Pipeline – Alec Russell, The Telegraph

Soviets Burned by CIA Hackers? – Wired

U.S. Revives Secret Program to Sabotage Iranian Missiles and Rockets – David E. Sanger and William J. Broad, The New York Times

Successful Sabotage of Drone Highlights Additive Manufacturing Security Needs – Karen Haywood Queen, Advanced Manufacturing

Pentagon is Rethinking its Multibillion-Dollar Relationship with U.S. Defense Contractors to Boost Supply Chain Security – Ellen Nakashima

Dragos Oil and Gas Threat Perspective Summary – Dragos

ICS Cybersecurity: You Cannot Secure what you Cannot See – David Zahn, PAS

Federal Investigators Pinpoint what Caused String of Gas Explosions in Mass. – Merrit Kennedy, NPR

Enbridge Needs U.S. Approval to Restart Natgas Pipe after Kentucky Blast – Reuters

Safety Recommendation Report – Natural Gas Distribution System Project Development and Review (Urgent) – US National Transportation Safety Board

Türkische Pipeline-Explosion wohl kein Cyber-Angriff – Hakan Tanriverdi, Suddeutsche Zeitung

Closing the Case on the Reported 2008 Russian Cyber Attack on the BTC Pipeline – Rob M. Lee, SANS

Attack on Natural Gas Network Shows Rising Cyberthreat – Blake Sobczak, E&E News

The Four Types of Threat Detection with Case-Studies in Industrial Control Systems (ICS) – Sergio Caltagirone and Robert M. Lee, Dragos

Indicators vs. Anomalies vs. Behaviors: A Critical Examination for ICS Defense – Joe Slowik (CS3STHLM Conference)