THE CYBER-PHYSICAL SIX

How targeted industrial attacks have evolved and a prediction of what's to come

HONEYWELL GLOBAL ANALYSIS, RESEARCH, AND DEFENSE (GARD)

EXECUTIVE RESEARCH REPORT

Ganesh Gadhe

Eric D. Knapp

Jim Lentz

Steve Ypma

Doug Swain

David Young

Honeywell

TABLE OF CONTENTS

INTRODUCTION

For many years the concept of a cyber-physical attack — where a cyber attack on digital systems is able to produce a physical impact — was something imagined, and perhaps feared. In 2010, The world was introduced to the first real example of a cyber-physical attack. New malware had been discovered that could sabotage a physical process by manipulating process control logic: Stuxnet. News of Stuxnet spread around the world via the mass media throughout the fall of 2010 for being the first threat of its kind: highly sophisticated, using multiple zero-days, with a large and complex code base, capable of propagating quickly and adapting to its environment until it found a very specific target. Once it found that target (a specific controller connected to a specific model of centrifuge operating under specific parameters), it caused the motors to operate under conditions that resulted in a physical failure. For the first time, malware was able to cause physical destruction.

Since Stuxnet, there have been numerous cyber-attacks against industrial control (often referred to as "OT" or "Operational Technology"). Five such attacks are classified as "cyber-physical" attacks. Like Stuxnet, they are designed to cause physical impact via cyber means. The first, BlackEnergy, caused prolonged blackouts in Ukraine in 2015, and a year later in 2016, Industroyer targeted Ukraine's energy grid once again.

In 2017, Trisis shocked the world again by targeting safety instrumented systems (SIS) for the first time, threatening to undermine the safety controls that might otherwise limit the physical impact of a cyber-attack. In April 2022, two different cyber-physical attacks were discovered: Industroyer 2, targeting Ukraine's grid for a third time; and Incontroller, a new and highly advanced cyber-physical attack platform capable of impacting a broad range of industrial controls including SIS.

At the time of this report, these six are the only known cyber-physical attacks. However, each of the six is enormously important and each represents a significant threat to process industries.

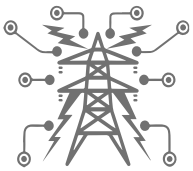
The "Cyber-Physical Six", individually, warrant close study by anyone looking to secure an industrial or OT environment. This report will not go into detail on any one of these attacks, as they have already been researched thoroughly. This report combines recent observations from Honeywell's GARD threat research team with more general observations about these six cyber-physical attacks. By looking at them together, they highlight some key trends that help us understand how an attacker might develop additional cyber-physical attacks and make predictions about what future attacks might look like.

STUXNET
2010

"...Malware of unprecedented complexity... the most sophisticated piece of malicious code known to man" [1]

BLACK ENERGY
2015

"This attack was exceptionally well organized and executed, but the tools necessary to mitigate and minimize the impact of as this are not difficult to implement" [2]



INDUSTROYER
2015

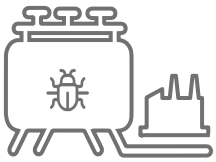
"Industroyer is a particularly dangerous threat, since it is capable of controlling electricity substation switches and circuit breakers directly"[3]

TRISIS
2017

"A rare and dangerous new form of malware targets the industrial safety control systems that protect human life" [4]

INDUSTROYER 2
2022

" Industroyer V2 reinforces the notion that OT malware can be tailored for use against multiple victims, which has serious implications..." [5]



INCONTROLLER
2022

Incontroller represents an exceptionally rare and dangerous cyber attack capability...

Incontroller was built to manipulate and disrupt industrial processes " [6]

THE HISTORY OF CYBER-PHYSICAL ATTACKS

Each of the Cyber-Physical Six represents an evolution from the attacks that preceded it. By looking at how each one changed, some obvious trends emerge in both attack capability and complexity. While all cyber-physical attacks can cause physical destruction, the overall capability of each differs in terms of usability, adaptability, and precision.

STUXNET

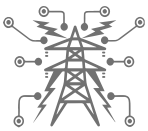
In its time, Stuxnet was lauded for its massive code base and ability to adapt, target, and destroy using novel, complex and adaptive malware to spread quickly, examining each infected target until the discovery of specific software with specific configurations informed it that it had found its intended industrial target. At that point, Stuxnet attacked that target with the intent to destroy it. It was extremely targeted, looking for a Siemens SIMATIC system that utilized specific Programmable Logic Controller (PLC) models running specific configurations. It leveraged knowledge of the SIMATIC system as well as the Profibus protocol used by that system to manipulate the behavior of targeted centrifuges, causing them to fail[7]. One important quality of Stuxnet is that it was unguided: that is, it did not require a command-and-control (C2) capability back to the threat actor. Instead, the malware itself observed and adapted, allowing it to spread broadly, only initiating the cyber-physical stages of the attack once it had identified a suitable target. While this was an effective strategy, the malware itself was widespread and therefore "noisy" — Stuxnet had infected over a hundred thousand systems in 155 countries[8] within a year of its initial detection, and as such the malware has been thoroughly analyzed and communications with C2 servers have been thoroughly observed.

Since Stuxnet, we've seen patterns of increased capability and refinement of purpose. Five additional industrial cyber-attack frameworks of greater capacity have been discovered since Stuxnet, likely learned from earlier attacks and, in some cases (such as Industroyer and Industroyer 2) with clear evidence that new attacks were built directly from the source code of their predecessors. Examining the history of cyber-physical threats provides valuable insight into how they have evolved. All six — Stuxnet, BlackEnergy, Industroyer, Trisis, Industroyer 2, and Incontroller — can cause their targets to produce an unintended physical outcome, but via different means. Looking at them in sequence, we see some clear patterns emerge.

BLACKENERGY

In 2015, a highly coordinated attack campaign showed how multiple targets could be manipulated in unison to create a much greater impact: the use of legitimate user credentials and remote access methods to access HMIs and use them to manipulate circuit breakers, while operators watched helplessly; the use of destructive malware to disable industrial control systems and damage the network infrastructure needed to access the breakers; the scheduled disconnection of Uninterruptable Power Supplies to further hinder response capability; and a Denial-of-Service attack on telecommunications infrastructure to thwart a coordinated response.[9] The malware used included the remote access trojan "BlackEnergy 3", hence, attack campaign itself is often referred to as BlackEnergy.

While the malware itself wasn't overly sophisticated, a coordinated attack combining with misuse of credentials resulted in extended blackouts across three distribution areas. In other words, BlackEnergy was more a successful exercise in figuring out a concerted attack strategy than developing an attack framework.



INDUSTROYER

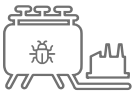
The cyber-physical threat landscape changed again just a year later with the discovery cyber-physical attack framework. Industroyer was configurable and included four modules, each designed to manipulate one of four industrial protocols: IEC 60870-5-101, IEC 70870-5-104, IEC 61850, and OLE for Process Control Data Access (OPC-DA)[10]. Rather than requiring legitimate accounts to manipulate the industrial control process as an authorized user, Industroyer could be installed on a system within the industrial network, and then leverage the industrial protocols themselves to manipulate process control directly. Industroyer was able to deliver configurable payloads but was dependent upon active command-and-control (C2) communication to do so.

TRISIS

A year after Industroyer came Trisis, the first malware to target a Safety Instrumented System (SIS), the implications of which are enormous: cyber-physical attacks are designed to cause a physical disruption, and a well-designed system will incorporate safety controls to prevent hazardous physical conditions from occurring. Thus, the potential to disrupt or disable those controls could enable the full physical impact of a cyber-physical attack. The malware itself, however, was very simple: a compiled python script with two embedded executables, and two externally linked executables. The embedded components enable Trisis to replace SIS controller logic, and the external components provide the new logic with which to replace it.[11] At a high level, Trisis is only novel in its targeting of SIS. To be effective, it still requires an enormous amount of early-stage attack activity. That is, the attacker must first understand the target infrastructure, and successfully install a command-and-control capability within that environment. Because Trisis needs to operate from a system that is capable of communicating with the target SIS controller, this initial attack stage will require more effort to reach the SIS. Once the adversary has a foothold on its target, however, information about the specific target SIS device(s) can be obtained and customized logic can be delivered to the SIS controllers. Unlike Industroyer, the cyber-physical effects of Trisis are the result of altered controller logic, rather than manipulation of industrial protocols.

INDUSTROYER 2

Industroyer 2 is a newer variant of Industroyer discovered in 2022, six years after its predecessor and five years after Trisis. While one might expect a new version to be more complex, perhaps with additional protocol modules, the opposite is true: Industroyer 2 is actually much simpler. It uses just one of the modules from its predecessor (IEC-104), in a single executable. The configuration functions are still present, but hard coded into that same executable. Unlike other cyber-physical threats, Industroyer 2 does not utilize any C2 capabilities.[12] If introduced to a target environment that aligns with its configuration, it can operate on its own. It is therefore simpler to deploy, and just as effective (assuming the adversary has sufficient intel on the target environment to configure the executable correctly). Therefore, we can speculate that Industroyer 2 is more of a refinement than an evolution of the framework itself. With data gathered from earlier deployments of Industroyer (or via other means) the necessary configurations can be made confidently, resulting in an effective self-contained attack capability. It is also easy to suppose that additional packaged variants of Industroyer's remaining modules (IEC-101, 61850, and OPC-DA) could be leveraged in a similar manner.



INCONTROLLER

Incontroller, also known as Pipedream, was identified in April 2022. Incontroller introduces a new cyber-physical attack framework that is even more capable, flexible, and advanced than previous frameworks. Incontroller combines several capabilities that include initial reconnaissance of industrial environments, establishment of backdoors and remote access for C2, direct manipulation of specific controllers and direct manipulation of industrial protocols. Incontroller is especially interesting in that it can directly leverage industrial protocols including OLE for Process Control Unified Architecture (OPC-UA) and Modbus, popular protocols used across a variety of industrial sectors. In addition, Incontroller includes modules to target specific PLC models, showing how the framework can pose a greater threat against specific targets.[13] While the devices targeted are used across several industries, researchers at Dragos assess that the likely targets include both electric power and Liquefied Natural Gas (LNG).[14]

Incontroller, fortunately, has not been directly associated with a cyber-physical incident at the time of this writing. However, in the initial analysis provided by Mandiant and Schneider Electric, it was determined that "Incontroller represents an exceptionally rare and dangerous cyber-attack capability," and that the flexibility of Incontroller enables a variety of attack scenarios that include the disruption of controllers to shut down operations, the reprogramming of controllers to sabotage industrial processes, and the disabling of safety controllers to cause physical destruction.[15]

These six cyber-physical attack capabilities have only been summarized here at the highest level; however, each represents an important aspect of industrial cybersecurity and readers are encouraged to study original research reports cited here, including reports from: Langner, Inc.; Symantec, Booz Allen Hamilton Inc; Mandiant; ESET; and others. Also note that a seventh industrial attack campaign, Dragonfly, was purposefully omitted from this report: while it did target industrial control and can enumerate targets leveraging the OPC protocol, it was used exclusively for reconnaissance rather than a cyber-physical impact, and so is not considered a cyber-physical threat.

OBSERVATIONS & TRENDS

While there are only six examples of cyber-physical attack campaigns to observe, there are still noticeable trends, including:

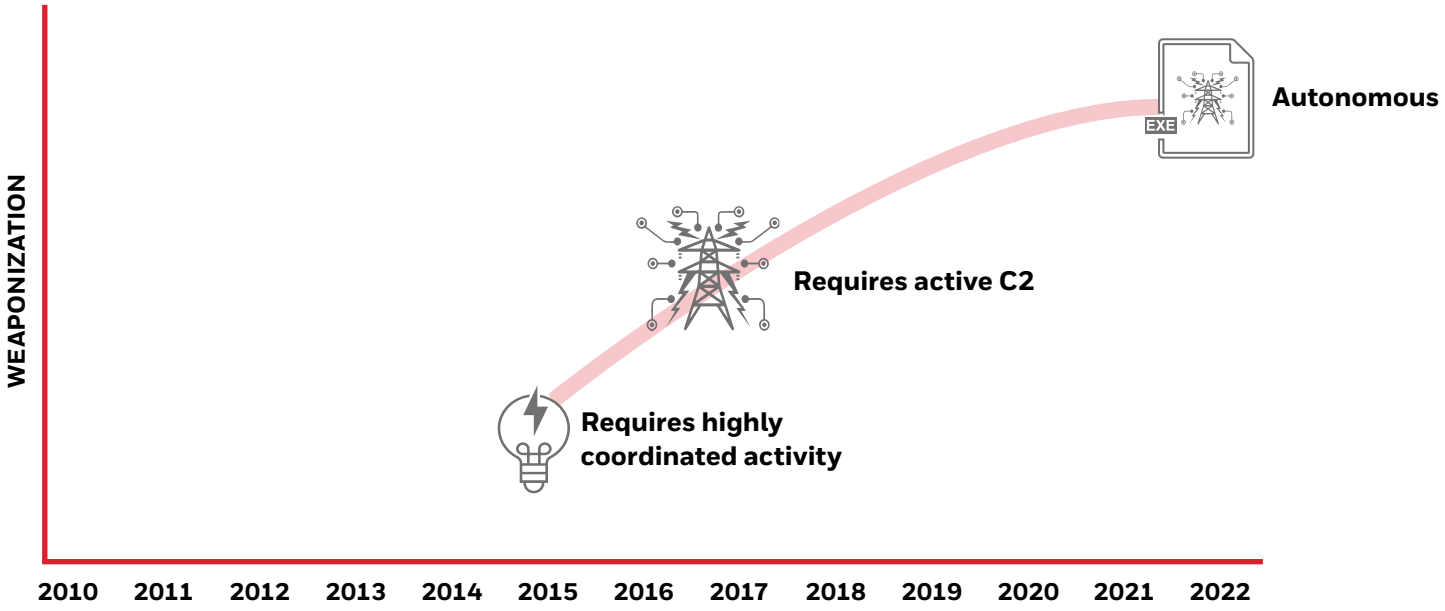
1. Broad capabilities that are highly dependent on C2 communications are developed first, using modular frameworks, followed by more refined implementations with more specific targets.
2. There is a consistent need for penetration of the industrial network, using initial attack phases that rely on a few consistent vectors: network penetration (typically via initial intrusion of business networks); removable media such as USB thumb drives; and the supply chain.
3. There is a steady increase in the overall attack surface. With each new attack comes a net increase in the overall cyber-physical threat capability.
4. There is a quickening pace of development, with a dwindling delay between new cyber-physical attacks.

1. MODULARITY vs. WEAPONIZATION

To uncover trends in the evolution of cyber-physical threats, the first area of focus is on BlackEnergy, Industroyer, and Industroyer 2. All of these threats shared a common target: energy distribution in Ukraine. The use of common code between the Industroyers, and other similarities including the use of common wiper malware, has caused many to speculate that all three attacks originated from the same adversary[16], and illustrates how an attack campaign against a given target evolved over several years.

What we see here is a clear trend of:

- Developing a capability (learning what to do and how to do it) focusing on how to disrupt distribution using the HMI. (BlackEnergy)
- Creating a modular framework with which to obtain target information and deliver targeted payloads. (Industroyer)
- Creating a more refined and automated threat package to simplify and streamline the threat. (Industroyer 2)



A clear trend of increased refinement and capability

2. CYBER-PHYSICAL THREATS AND INDUSTRIAL ATTACK VECTORS

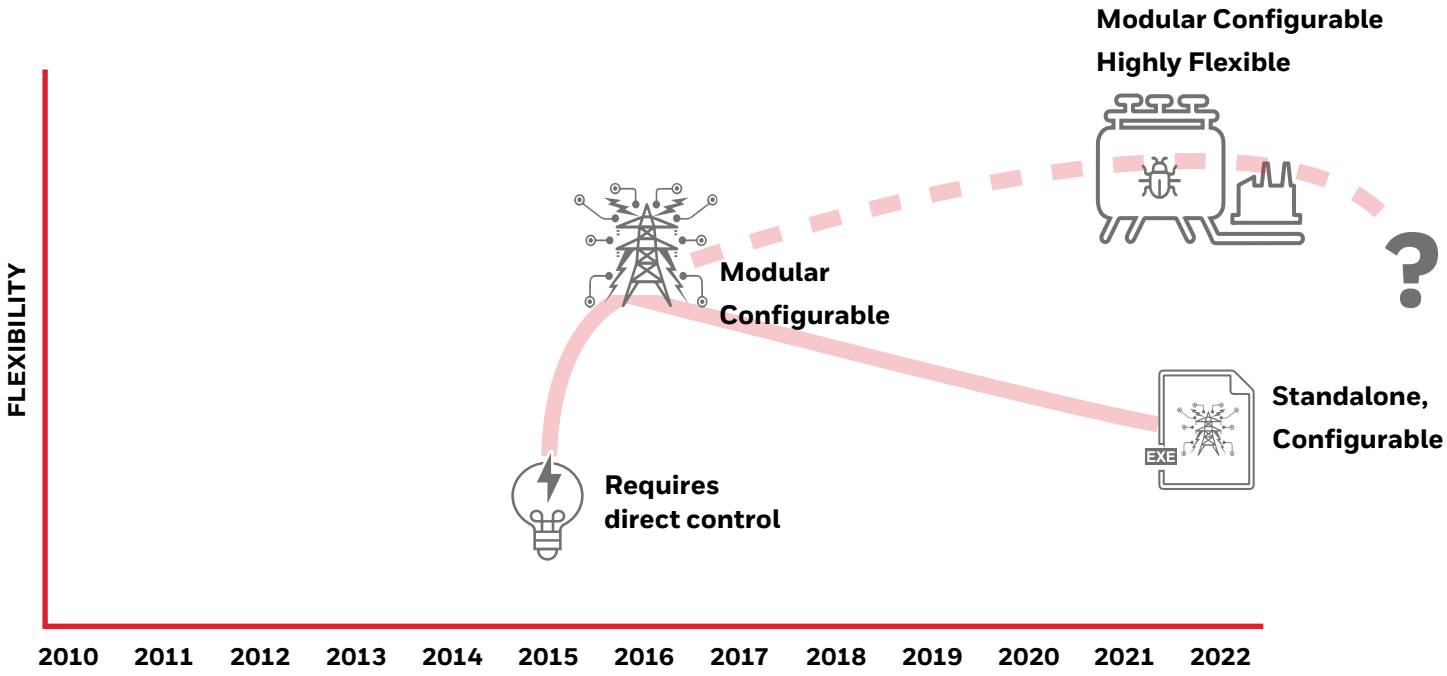
Other recent threat data highlights activity leveraging the two primary attack vectors into industrial control environments: network communications and removable media.

In 2018, Honeywell began publishing an annual USB Industrial Cybersecurity Threat Report to examine the USB attack vector in more depth. This report is unique in that it focuses exclusively on threats that were detected and blocked on removable media while entering an industrial control facility by leveraging telemetry from Honeywell's Secure Media Exchange (SMX) gateways deployed across all 16 critical infrastructure sectors, and across 55 countries.

While it is well known that the first of the Cyber-Physical Six, Stuxnet, leveraged USB media as an initial attack vector, all of the cyber-physical attacks discussed here are capable of leveraging this vector as well. From the USB threat research conducted between 2019 to 2023, Honeywell consistently saw that approximately half of all malware found on removable media was designed specifically to propagate via USB and/or leveraged aspects of USB media in order to execute. This indicates an awareness among adversaries that portable media such as USB thumb drives remain an effective vector, especially into isolated environments such as industrial control systems, which may be more difficult to reach via the network. Some of the relevant findings from Honeywell's

USB Threat Reports include:

- The amount of media-borne malware that included C2 capabilities, including data exfiltration and remote access, rose from 44% in 2019 to 72% in 2023. This is an important observation due to the dependence of cyber-physical attack frameworks have on C2.
- Malware associated with Stuxnet, BlackEnergy, Industroyer, Industroyer 2, and Trisis has been successfully detected and blocked on removable media since 2019, indicating that removable media remains an active vector for these campaigns. (Note that the 6th, Incontroller, has not been deployed successfully in the wild, and there are no disclosed indicators to detect as of the time of this report).



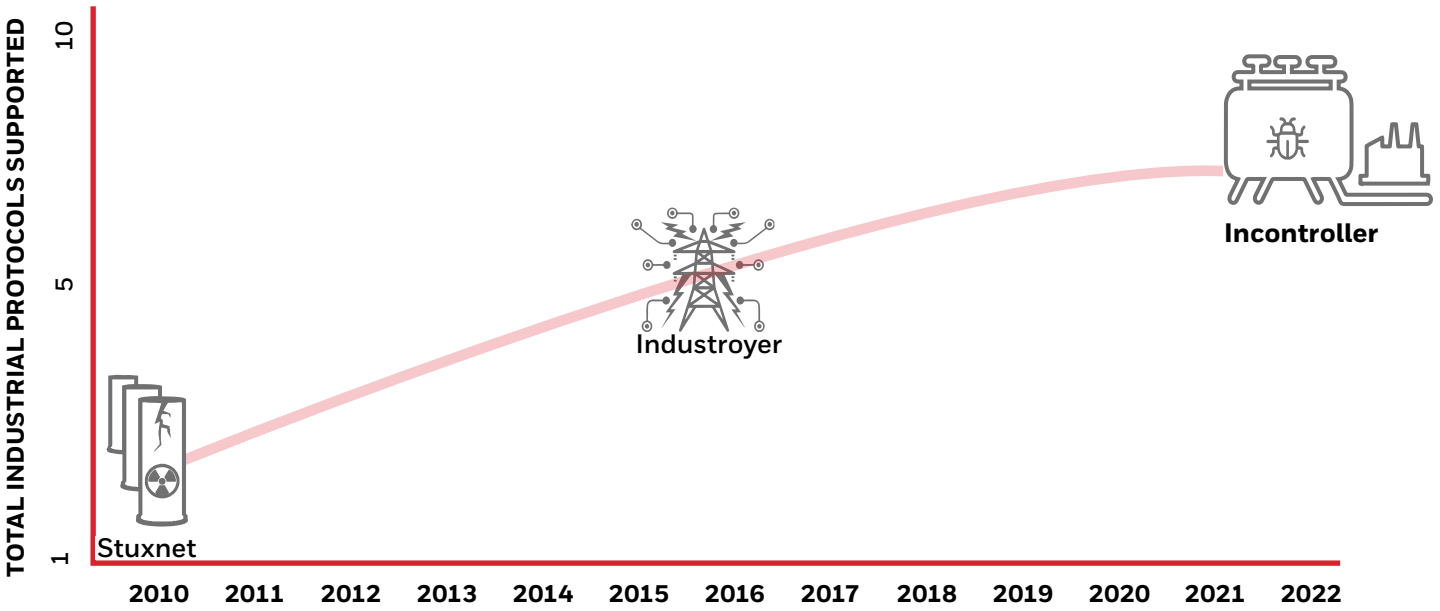
Modular frameworks evolve, while also driving new specialized variants

3. EXPANDING CAPABILITIES

Each of the Cyber-Physical Six introduces new devices that can be targeted; in some cases, entire device categories can be targeted via the direct manipulation of industrial protocols. The result is that with each new attack comes a net increase in the overall cyber-physical threat capability. Simply put, more tools are available within an adversaries' toolkit. Because cyber-physical threats are now present in the form of modular and configurable frameworks, adversaries can use various capabilities as needed to create a total cyber-physical threat capable of attacking a considerable percentage of industrial operations.

INDUSTRIAL PROTOCOLS SUPPORTED BY CURRENTLY KNOWN CYBER-PHYSICAL ATTACK PLATFORMS		
Profibus [17]	OPC-DA [20]	IEC 60870-5-104 [23]
Modbus [18]	IEC 61850 [21]	FINS [24]
OPC-UA [19]	IEC 60870-5-101 [22]	Codesys [25]

While not all-inclusive, this provides broad coverage of energy and utilities, manufacturing, oil & gas, and building automation industries. OPC alone "is the most widely adopted interoperability standard for secure, reliable and platform-independent information exchange in the world", according to the OPC Foundation.[26] Modbus and Profibus protocols are used in approximately 18% of industrial networks, [27] extending the attack surface even further.



Building upon previous capabilities, the number of industrial protocols that can be directly manipulated continues to grow

4. FREQUENCY OF NEW CYBER-PHYSICAL ATTACK CAPABILITIES

The final trend is perhaps the most obvious. There was a 5-year gap between Stuxnet in 2010 and BlackEnergy in 2015. Then, two more of the Cyber-Physical Six were introduced annually in 2016 and 2017. The gap following Trisis in 2017 was just under five years, with the remaining two (Industroyer 2 and Incontroller) hitting at almost the same time in early 2022.

In the time of Stuxnet, cyber-physical attacks were novel. Now, there is a wealth of research for cyber adversaries to build upon, and more existing capability with each new attack. At the Black Hat USA conference in 2010 – the same year that Stuxnet introduced the world to a real cyber-physical attack for the first time – there was a single presentation on SCADA and ICS security that largely mocked the concept as "FUD" (Fear Uncertainty and Doubt).[28] In 2022, the same conference held an entire session track on cyber-physical security, and renowned journalist Kim Zetter gave a keynote on the subject of Stuxnet, cyber war, and the state of industrial cybersecurity.[29]

Will this trend continue? Only time will tell. If it does, we can expect additional cyber-physical attacks to emerge in the immediate future, before a diminishing gap of perhaps three to four years as new capabilities are developed into a new batch of even more capable cyber-physical attack frameworks.

UNDERSTANDING OT ATTACK VECTORS

To manipulate the control system — either through access to and utilization of HMI, replacement of control logic, or manipulation of industrial control protocols — first requires access to the industrial control network where target controllers are deployed. In a properly designed environment, this limits the potential vectors that an adversary can utilize in the initial attack phase:

1. **The Network**
   By first breaching business network(s), or utilizing remote access paths, adversaries require initial network penetration using traditional network attack techniques before pivoting into lower levels of the industrial networkOnce inside the industrial environment, adversaries can establish remote access to C2 servers, enabling cyber-physical attack phases.

2. **Removable Media**
   A common method of transferring data and files into and out of an industrial control environment is via removable media such as USB thumb drives. Attacks leveraging removable media can bypass network security controls, making it a popular attack vector against isolated OT systems.

3. **The Supply Chain**
   Both the hardware and software supply chain represent potential vectors into industrial networks. Hardware supplies are physically carried in past network defenses and could include devices that have been tampered with the intent of establishing covert networks for C2 or other malicious purposes. Several USB attack platforms could be introduced via the hardware supply chain, disguised as other legitimate devices (please refer to the Honeywell USB Hardware Attack Platforms Report).

TAKEAWAYS & GUIDANCE

Every one of the Cyber-Physical Six requires extensive intelligence about its target, to determine what types of industrial assets are in use, how automation logic is used, what safety controls or redundancies might be in place, etc. This means that an attacker requires extensive reconnaissance and intelligence gathering, and/or a reliable Command and Control (C2) system in place to enumerate target systems and exfiltrate the required information. For C2, a network connection is required, which in turn requires a preliminary attack stage to penetrate the industrial target to install a backdoor. Without effective C2, an attacker must rely on intelligence gathering via other means.

1. Protect the information that attackers require. This includes any sensitive information, from relevant business data to process control logic. An attacker could use asset inventories, procurement records, digital system backups, etc. to determine the process control architecture, assets, and automation functions required to develop a targeted cybyer-physical attack.
2. Implement security controls on "beach-head" systems that an attack might be able to compromise within process control networks. This could be systems that an attack could potentially 'pivot' to from the business network, or systems with USB interfaces that could potentially be used to penetrate the industrial control network.
3. Implement tight security controls on all network traffic, but especially outbound network traffic to prevent unauthorized backdoors and Remote Access Trojans from successfully reaching C2 servers operated by threat actors.

Once they have access to industrial control networks, newer Cyber-physical attacks leverage process control to achieve their goals, rather than depending upon specific device or software vulnerabilities. Attackers did not need to find process and SIS controllers that were unpatched or possessing some firmware vulnerability; the target devices were functioning as designed and were suspectable because of the ability to manipulate industrial protocols and process logic.

1. Prioritize vulnerability scanning and patching efforts where they are most effective: with higher priorities for general computing systems and servers deployed at higher levels of the Purdue model, and lower priorities for controllers, PLCs, SIS, and other assets deployed at lower levels of the Purdue model. While all patching is important, do not delay the patching of higher priority systems to include systems that are lower priority (and typically much harder to patch).
2. Assume that all industrial control assets are vulnerable. Because an industrial control system is capable of being misused as a system, the system itself represents a vulnerability even when all assets are fully hardened and patched. Monitor the process and leverage observed activities of the process alongside other cybersecurity monitoring and controls to detect cyber-physical attack phases.

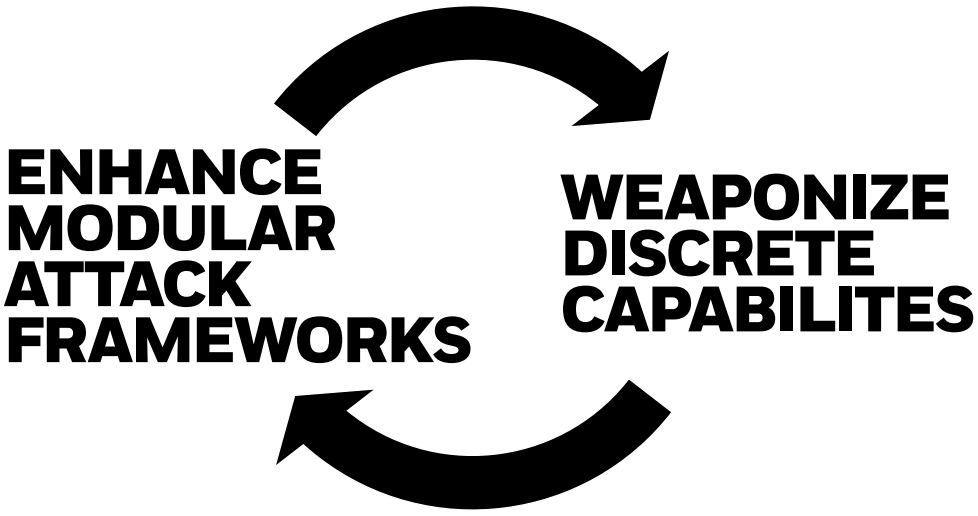
Electric utilities are not the only ones at risk. While many of the cyber-physical attacks have targeted electric distribution, the target of the most concerning framework, Incontroller, is currently unknown. The capacity to manipulate modular and flexible frameworks such as OPC-UA, Modbus, Codesys, and FINS represent a broad scope of addressable targets across several industries with the potential to expand.

1. If using any of the currently targeted industrial protocols, ensure that all associated networks are segmented and protected. Where available (e.g., OPC-UA) enable all available security functions including encryption, authentication, and access control.
2. Consider the potential risks of malicious or unintended control commands and design your control system with resiliency to minimize the impact of a cyber-physical incident should one occur.
3. Remember that SIS controls could be manipulated as well. Ensure adequate segmentation of SIS equipment into distinct zones, with adequate controls on all SIS-related data flows.

WHAT WE CAN EXPECT

With Incontroller, we have a new blueprint for developing a coordinated cyber-physical campaign. Just as Industroyer enabled more concise, targeted payloads such as those found in Industroyer 2, we can expect the same here. Incontroller is modular and flexible; the components can be coordinated or piecemeal. As with Industroyer, successful deployment of Incontroller would provide greater exposure to industrial systems via both the OPC-UA and DNP-3 protocols. With enough reconnaissance of this type, adversaries could develop more concise and packaged cyber threats to disrupt, manipulate, or destroy specific targets.

Similarly, while the addressable target space for cyber-physical attacks is already significant, the protocols leveraged by current cyber-physical attack frameworks were likely chosen because of their prolific use within the energy industry. However, additional industrial protocols could be leveraged to target additional industrial sectors, and the currently supported protocols are used in other industries than energy. In other words, the potential applications of existing frameworks have yet to be exhausted, and the ability to extend the current frameworks to support entirely new use cases is real.



CONCLUSION

Today's cyber-attack capability is real and has been proven effective. The six cyber-physical attacks known to date represent a real threat to industrial operators, with the ability to disrupt, sabotage or destroy. Together, they represent a compound threat capable of targeted, disruptive attacks against various critical industries. The Cyber-Physical Six also highlight an evolutionary path that suggests the overall cyber-physical threat capability will continue to increase in capability and scope. A cybersecurity plan should include serious consideration for current and potential future-state threats.

The good news is that there are ways to mitigate these threats. The nature of industrial control and automation systems requires attackers to fully understand their targets before a cyber-physical attack can be successful. Providing strong IT security controls outside of OT environments can help prevent reconnaissance that can be used to develop a targeted attack. Properly segmenting industrial systems and implementing strong security controls across all attack vectors can make it difficult for adversaries to access industrial systems, helping to impede reconnaissance efforts and cyber-physical attack phases. Finally, understanding cyber-physical threats and improving the resiliency of the ICS to minimize physical impacts can impair a cyber-physical attack's ability to cause harm.

Cyber-physical attacks still require an initial attack phase to gain access to the industrial network. The limited vectors in industrial networks provides an opportunity to detect and prevent cyber-physical campaigns early.

Because all control systems are different, cyber-physical attacks still require extensive reconnaissance and planning, and/or active C2 channels, again providing an opportunity to detect and prevent cyber-physical campaigns early.

Cyber-physical threats are evolving from targeting specific assets to the manipulation of the ICS protocols, making them more flexible and reusable.

Cyber-physical threats are growing more powerful and flexible: deployable as an end-to-end attack frameworks, or as more refined & automated attack capabilities.

Cyber-physical threats are evolving to expand their viable attack surface, by leveraging more widely used protocols such as 61850, OPC, Modbus, and others.

GLOSSARY

Attack Vector
An attack vector is a path or method used by an attacker to exploit vulnerabilities in a system, network, or application — often with malicious intent.

BlackEnergy
BlackEnergy refers to a modular malware toolkit initially discovered in 2007. BlackEnergy 3 includes features like DDoS attacks, data exfiltration, and destruction of system data, and is notable for its use in the 2015 attack against the Ukrainian power grid. While 'BlackEnergy' technical refers to the malware, it is often used to refer to the attack campaign itself.

Command and Control (C2, C&C)
Command and Control refers to the communication channel between a compromised system or device and the attacker's server, enabling the attacker to remotely control and issue commands to the infected system.

Cyber-Physical attack
A cyber-physical attack is a cyberattack targeting computer systems that control physical processes, such as industrial control systems (ICS) or critical infrastructure. These attacks aim to manipulate or disrupt the operation of physical equipment, potentially causing real-world damage, safety hazards, or significant service disruption.

Cyber-Physical Six
A reference to the first six known cyber-physical attacks; the only such examples at the time of this report. The Cyber-Physical Six consists of Stuxnet, BlackEnergy, Industroyer, Trisis, Industroyer 2, and Incontroller.

Dragonfly
Dragonfly is a cyber-espionage campaign that targeted energy companies and critical infrastructure systems. The attackers used phishing emails, watering hole attacks, and malware to gain unauthorized access and steal sensitive information about industrial control networks.

IEC 60870-5-101 (IEC-101)
IEC 60870 is a set of international standards developed by the IEC that define communication protocols and data formats for supervisory control and data acquisition (SCADA) systems commonly used in monitoring, controlling, and automating electrical power transmission and distribution networks. IEC 60870-5-101 is a protocol for point-to-point and point-to-multipoint serial communication.

IEC 60870-5-104 (IEC-104)
IEC 60870 is a set of international standards developed by the IEC that define communication protocols and data formats for supervisory control and data acquisition (SCADA) systems commonly used in monitoring, controlling, and automating electrical power transmission and distribution networks. IEC 60870-5-104 is a protocol for connecting remote devices and control centers of TCP/IP.

IEC 61850
IEC 61850 is an international standard developed by the IEC designed to improve the interoperability of protection, control, automation, and monitoring functions in power systems. IEC 61850 enables communication between circuit breakers, transformers, protection relays, and other devices in a substation.

Incontroller
Incontroller, also known as Pipedream, is the newest cyber-physical malware at the time of this writing. It is a highly flexible, modular threat that has the potential to target a wide variety of systems across multiple industries.

Industroyer
Industroyer, also known as CrashOverride, is a cyber-physical malware that targets industrial control systems used in electric distribution. Industroyer's modular design enables it to target various communication protocols, making it more flexible and reusable than previous cyber-physical attack frameworks.

Industroyer 2
Industroyer 2 is a cyber-physical malware derived from Industroyer. Like Industroyer, Industroyer 2 targets industrial control systems used in electric distribution. However, Industroyer 2 only supports one protocol and is contained within a single executable.

Modbus
Modbus is a communication protocol for industrial devices used in industrial automation and control systems. It allows data exchange between a central controller and multiple devices. It can operate over serial (RS-232, RS-485) and TCP/IP.

OLE for Process Control Data Access (OPC-DA)
OPC-DA is a protocol enabling real-time data exchange between industrial devices and software applications, developed by the OPC Foundation. It uses Microsoft's COM and DCOM technologies for communication, providing a standardized interface for accessing process data in automation systems.

OLE for Process Control Unified Architecture (OPC-UA)
OPC-UA is more modern and capable OLE process control protocol. Unlike OPC-DA, it is platform-independent, and includes security features encryption, authentication and access control. It also provides enhanced data modeling to provide interoperability across industries.

Profibus
Profibus (Process Field Bus) is a widely used industrial communication standard for automation and process control systems, developed by Siemens and other manufacturers. It enables data exchange between controllers, such as PLCs, and field devices, such as sensors and actuators, primarily in manufacturing and process industries.

Programmable Logic Controller (PLC)
A Programmable Logic Controller (PLC) is an industrial computer designed to control and automate manufacturing processes, machinery, or production lines. PLCs are rugged, reliable, and built to operate in harsh environments, using inputs from sensors and executing programmed logic to control outputs like motors, valves, or alarms

Safety Instrumented Systems (SIS)
Safety Instrumented Systems (SIS) are specialized control systems designed to ensure the safe operation of industrial processes by monitoring conditions and taking corrective actions if necessary. E.g., open a relief valve in response to unsafe pressure conditions.

Stuxnet
Stuxnet is a sophisticated computer worm that targeted industrial control systems. It is largely recognized as the first cyber-physical attack to be deployed outside of a lab. It was designed to sabotage Iran's nuclear program by causing physical damage to centrifuges used for uranium enrichment.

Trisis
Trisis is a cyber-physical malware, the first known malware to target Safety Instrumented System (SIS) controllers.

Zero-day
A zero-day attack is an exploitation of a previously unknown vulnerability in software, hardware, or firmware. Because the exploits and associated vulnerabilities are unknown, zero-day attacks can be particularly dangerous and difficult to detect.

ABOUT GLOBAL ANALYSIS RESEARCH AND DEFENSE (GARD)

Proactive threat research helps ensure that targeted OT threats are detected early. Honeywell's Global Analysis, Research, and Defense team (GARD) is dedicated to OT focused cybersecurity research, innovation, and integration. As part of Honeywell OT Cybersecurity, GARD leverages data curated from 7 Honeywell cybersecurity research centers, and from thousands of deployments in over 65 countries – to provide OT threat analysis and threat detection.

Honeywell OT Cybersecurity is a Honeywell business dedicated to better protecting industrial assets, operations and people from digital-age threats. With more than 15 years of OT cybersecurity expertise and over 50 years of industrial domain expertise, Honeywell combines proven cybersecurity technology and industrial know-how to maximize productivity, improve reliability and increase safety. We provide innovative cybersecurity software, services and solutions to better protect assets, operations and people at industrial and critical infrastructure facilities around the world.

REFERENCES

1. Ralph Langner. Stuxnet analysis by Langner. Cited 3/15/23. https://www.langner.com/stuxnet/
2. Ake Styczynski, Nate Beach-Westmoreland. When The Lights Went Out: A Comprehensive Review of the 2015 Attacks on Ukrainian Critical Infrastructure. Booz Allen Hamilton Inc. 2019
3. Robert Lipovsky, Anton Cherepanov. ESET. Industroyer: Biggest threat to industrial control systems since Stuxnet. June 12, 2017. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/
4. Andy Greenberg, WIRED. Unprecedented Malware Targets Industrial Safety Systems in the Middle East. Dec 14, 2017. https://www.wired.com/story/triton-malware-targets-industrial-safety-systems-in-the-middle-east/
5. Daniel Kapellmann Zafra, Raymond Leong, Chris Sistrunk, Ken Proska, Corey Hildebrandt, Keith Lunden, Nathan Brubaker, INDUSTROYER.V2: Old Malware Learns New Tricks. April 25, 2022. Updated December 02, 2022. Mandiant. https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks
6. Nathan Brubaker, Keith Lunden, Ken Proska, Muhammad Umair, Daniel Kapellmann Zafra, Corey Hildebrandt, Rob Caldwell. INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems. Mandiant. April 13, 2022. https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool
7. Ralph Langner. To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. The Langner Group. November 2013. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
8. Symantec. W32.Stuxnet Dossier. November 2010. Archived from the original (PDF) on 4 November 2019. https://web.archive.org/web/20191104195500/https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
9. Ake Styczynski, Nate Beach-Westmoreland. When The Lights Went Out: A Comprehensive Review of the 2015 Attacks on Ukrainian Critical Infrastructure. Booz Allen Hamilton Inc. 2019
10. Cherepanov, Anton. Industroyer: Biggest threat to industrial control systems since Stuxnet. www.welivesecurity.com. ESET. June 17, 2017.
11. Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, Christopher Glyer. Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure. Mandiant Threat Research. Dec 14, 2017. Cited March 2023. https://www.mandiant.com/resources/blog/attackers-deploy-new-ics-attack-framework-triton
12. Welivesecurity, by ESET. Industroyer 2: Industroyer reloaded. This ICS-capable malware targets a Ukrainian energy company. April 12, 2022. ESET Research. https://www.welivesecurity.com/2022/04/12/Industroyer 2-industroyer-reloaded/
13. Nathan Brubaker, Keith Lunden, Ken Proska, Muhammad Umair, Daniel Kapellmann Zafra, Corey Hildebrandt, Rob Caldwell. INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems. Mandiant. April 13, 2022. Cited March 2022. https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool
14. Dragos, Inc. Pipedream: Chernovite's Emerging Malware Targeting Industrial Control Systems. April, 2022.
15. Ibid.
16. Anton Chereppanov, Robert Lipovsky. Industroyer 2: Sandworm's Cyberwarfare Targets Ukraine's Power Grid Again. Black Hat USA 2022.
17. Ralph Langner. To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. The Langner Group. November 2013. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
18. Nathan Brubaker, Keith Lunden, Ken Proska, Muhammad Umair, Daniel Kapellmann Zafra, Corey Hildebrandt, Rob Caldwell. INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems. Mandiant. April 13, 2022. Cited March 2022. https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool
19. Ibid.
20. Cherepanov, Anton. Industroyer: Biggest threat to industrial control systems since Stuxnet. www.welivesecurity.com. ESET. June 17, 2017.
21. Ibid.
22. Ibid.
23. Ibid.
24. Nathan Brubaker, Keith Lunden, Ken Proska, Muhammad Umair, Daniel Kapellmann Zafra, Corey Hildebrandt, Rob Caldwell. INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems. Mandiant. April 13, 2022. Cited March 2022. https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool
25. Ibid.
26. OPC Foundation. https://opcfoundation.org/members. Cited March 22, 2022.
27. Industrial Ethernet Book. 2022 Industrial Network Market Shares according to HMS Networks. June 30, 2022. https://iebmedia.com/news/tech-updates/2022-industrial-network-market-shares-according-to-hms-networks/
28. James Arlen. SCADA and ICS for Security Experts: How to Avoid Cyberdouchery. Black Hat USA Conference, Las Vegas, August 2010.
29. Kim Zetter. Pre-Stuxnet, Post-Stuxnet: Everything Has Changed, Nothing Has Changed. Black Hat USA. Las Vegas, NV. Thursday Aug 11. https://www.youtube.com/watch?v=noNx1Dmo3K0

For more information
www.honeywellaidc.com

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 30308
www.becybersecure.com

THE FUTURE IS WHAT WE MAKE IT

Honeywell