U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Mario Garcia
Supervisory Cybersecurity Advisor
(Sacramento, California)

Presented at IEEE Consultants' Network of Silicon Valley (IEEE-CNSV)

Mario Garcia
June 13, 2023
Cybersecurity and Infrastructure Security Agency (CISA)

**VISION**
Secure and resilient infrastructure for the American people.

**MISSION**
CISA partners with industry and government to understand and manage risk to our Nation’s critical infrastructure.

**OVERALL GOALS**

**GOAL 1**
DEFEND TODAY
Defend against urgent threats and hazards

**GOAL 2**
SECURE TOMORROW
Strengthen critical infrastructure and address long-term risks
Critical Infrastructure Sectors

16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

- CHEMICAL: CISA
- COMMERCIAL FACILITIES: CISA
- COMMUNICATIONS: CISA
- CRITICAL MANUFACTURING: CISA
- DAMS: CISA
- DEFENSE INDUSTRIAL BASE: DOD
- EMERGENCY SERVICES: CISA
- ENERGY: DOE
- WATER: EPA
- FINANCIAL: Treasury
- FOOD & AGRICULTURE: USDA & HHS
- GOVERNMENT FACILITIES: GSA & FPS
- ELECTION INFRASTRUCTURE: 
- HEALTHCARE & PUBLIC HEALTH: HHS
- INFORMATION TECHNOLOGY: CISA
- NUCLEAR REACTORS, MATERIALS AND WASTE: CISA
- TRANSPORTATION SYSTEMS: TSA & USCG
- PIPELINE SYSTEMS: 

Mario Garcia
June 13, 2023
CISA Integrated Operations Division (IOD)

- CYBERSECURITY
- PROTECTIVE SECURITY
- CHEMICAL SECURITY
- EMERGENCY COMMUNICATIONS
- OPERATIONS & OUTREACH
ICS & OT Incidents

- Colonial Pipeline Attack – 2021
- NotPetya – 2017
- Stuxnet – 2010

https://www.cisa.gov/shields-up
Joint Cyber Defense Collaborative (JCDC-ICS)
“Control System Defense: Know the Opponent.” This NSA and CISA advisory breaks down the steps malicious cyber actors take to compromise critical infrastructure control systems so that you can better defend against them.

1. Establish intended effect and select a target
2. Collect intelligence about the target system
3. Develop techniques and tools to navigate and manipulate the system
4. Gain initial access to the system
5. Execute techniques and tools to create the intended effect
Reduce Exposure Across OT and CS

1. Have a Resilience Plan for OT
2. Exercise your Incident Response Plan
3. Harden Your Network
4. Create an Accurate “As-operated” OT Network Map Immediately
5. Understand and Evaluate Cyber-risk on “As-operated” OT Assets
6. Implement a Continuous and Vigilant System Monitoring Program
CISA ICS Offerings

- **Assessments**: Operational resilience evaluations
- **Cyber Hunt**: Aid ICS partners with adversary presence search in absence of known threat
- **Exercises**: Testing and readiness for ICS incidents
- **Information Exchange**: Sharing of threat and best practice guidance with partners
- **Partnerships and Engagement**: Collaborate and coordinate with ICS partners
- **Products and Tools**: Access to hands-on tools for the ICS community
- **Response**: Provide expertise and advanced tooling to aid ICS cyber victims
- **Strategic Risk Analysis**: Provide ICS risk information pertaining to National Critical Functions (NCFs)
- **Technical Analysis**: ICS malware analysis support
- **Training**: Technical and non-technical ICS instruction for all skill levels
- **Vulnerability Coordination**: Coordinated, public disclosure of ICS vulnerabilities + mitigation recommendations
CISA offers free cybersecurity services to Critical Infrastructure entities:

- **Vulnerability Scanning:** Persistent scanning of internet-accessible systems for vulnerabilities, configuration errors, and suboptimal security practices.

- **Web Application Scanning:** Assesses the “health” of publicly accessible web applications by checking for known vulnerabilities and weak configurations.

- **Phishing Campaign Assessment:** measures a workforce’s tendency to click on email phishing lures commonly used by cyber actors to collect sensitive information or to obtain initial access to a network.

- **CISA Assessments:** Agency cybersecurity assessments provide actionable and risk-informed recommendations. Email vulnerability@cisa.dhs.gov for more information and to sign up.
First of its kind cybersecurity grant program for state, local territorial and tribal governments across the country

$ 1 Billion over four years (2022 – 2025)

To help SLTT government leaders identify their cybersecurity needs, DHS created a Toolkit: [https://cisa.gov/cybergrants](https://cisa.gov/cybergrants)
Parting Thoughts …

- **Integrate** cybersecurity in your earliest designs and planning, and within each phase
  - Include IT and Cybersecurity Staff in your planning; they are not interchangeable
  - Consider your four types of assets: People, Information, Technology, Facilities
- Identify your critical service(s) and protect them and their dependencies
- Train for manual operation (Just because you have a calculator doesn’t mean you don’t have to know math!)
- Implement cybersecurity best practices (https://cisa.gov)
- Transnational Studies and Engagements
  - Keep sensitive information close to the vest
  - Know your international partners, consider vetting
  - Sharing should not be a one-way street

Everyone counts on IT to lead the response, but Incident Response is a shared and leadership driven event!
Contacts…

Mario Garcia
Supervisory Cybersecurity Advisor
Sacramento, CA
(202) 309-1847
Mario.Garcia@cisa.dhs.gov

CISA Region 9
Regional office: CISAR Region 9@cisa.dhs.gov

CISA Central 24/7
888-282-0870
Report incidents: Report@cisa.gov
Additional information: Central@cisa.dhs.gov
Cybersecurity for Industrial Control Systems

David Snyder, MBA, PE, CISSP, CCSP
IEEE Consultants Network of Silicon Valley

June 13, 2023
• Trained as a Civil Engineer
• Respiratory Therapy in hospital ICUs
• 20 years of environmental engineering, including electric power and petroleum industries and hazardous waste cleanup
• Switched to credit card systems 25 years ago
• E-commerce led to cybersecurity
• Currently a contractor at Apple in Public Key Infrastructure
• 42TEK LLC is my consulting practice
• Critical Infrastructure & Industrial Control
• Vulnerabilities & Attacks
• What We Can Do
## Critical Infrastructure Sectors

1. Chemical  
2. Commercial Facilities  
3. Communications  
4. Critical Manufacturing  
5. Dams  
6. Defense Industrial Base  
7. Emergency Services  
8. Energy  
9. Financial Services

10. Food and Agriculture  
11. Government Facilities  
12. Healthcare and Public Health  
13. Information Technology  
14. Nuclear Reactors, Materials, and Waste  
15. Transportation Systems  
16. Water and Wastewater Systems  

* Space Systems?
Industrial Control Systems

The term “industrial control systems” or “ICS” refers to a broad set of control systems, which include:

- SCADA (Supervisory Control and Data Acquisition)
- DCS (Distributed Control System)
- PCS (Process Control System)
- EMS (Energy Management System)
- AS (Automation System)
- SIS (Safety Instrumented System)
- Any other automated control system
Different Types of Industrial Control

- Process control, both continuous and batch – typically a Distributed Control System (DCS)
- Discrete control, sequence control – typically a Programmable Logic Controller (PLC)
- Remote monitoring and dispatch – typically a Supervisory Control and Data Acquisition System (SCADA)
- Life Safety or Personnel Protection – typically a Safety Instrumented System (SIS)

All Industrial Control Systems are designed for one primary purpose – and that is to automate a physical process. They accomplish this through sensors to measure physical properties and actuators to manipulate those properties.
• **Operational Technology (OT)** – is often used to describe Industrial Control Systems (ICS) and other “cyber physical systems” – but is also used to describe automation systems that aren’t industrial in nature but use similar technology
  • Building Automation Systems
  • Transportation (Avionics, Positive Train Control, etc.)
  • Medical Devices and systems (many CAT scan / MRI use PLC technology)

*Many of these systems have developed independently from ICS system development, but they look remarkably similar and have many of the same vulnerable sub-systems!*
Cybersecurity Differences

**IT**
- Data at rest
- Data in transit
- Confidentiality
- Integrity
- Availability

“computer science”

**ICS/OT**
- Things
- Actions
- Safety
- Reliability

“controls engineering”
Remote Terminal Unit

A remote terminal unit (RTU) is a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition) system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects.

A programmable logic controller (PLC) or programmable controller is an industrial computer that has been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, machines, robotic devices, or any activity that requires high reliability, ease of programming, and process fault diagnosis.

https://en.wikipedia.org/wiki/Programmable_logic_controller
Threat Modeling

• **What do we have?**  Asset inventory; process flow; network diagram
• **What can go wrong?** Risk assessment
• **What are we going to do about it?** Controls; mitigation measures
• **Did we do a good job?** Assessments; audits
Asset Inventories, Process Flows, and Piping & Instrument Diagrams
What Can Go Wrong?
Possible incidents an ICS may face

- **Blocked or delayed flow of information** through ICS networks, which could disrupt ICS operation.
- **Unauthorized changes** to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life.
- **Inaccurate information** sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects.

NIST Special Publication 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security
• ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects.

• Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment.

• Interference with the operation of safety systems, which could endanger human life.
VULNERABILITIES IN ICS

1. Easy connectivity
2. Plain text traffic and open protocols
3. Systems susceptible to buffer overloads (stack and heap) that have not been patched properly
4. Advanced features create more vulnerabilities
5. No authentication
6. Lack of embedded countermeasures
7. Dependence on underlying operating system
8. The use of contemporary IT countermeasures in ICS which do not necessarily work seamlessly together
9. DoS susceptible systems
10. Weak passwords

COMMON ICS CYBER VULNERABILITIES
<table>
<thead>
<tr>
<th>Threat Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial of Control Action</td>
<td>Control systems operation disrupted by delaying or blocking the flow of information, thereby denying availability of the networks to control system operators or causing information transfer bottlenecks or denial of service by IT-resident services (such as DNS)</td>
</tr>
<tr>
<td>Control Devices Reprogrammed</td>
<td>Unauthorized changes made to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers, alarm thresholds changed, or unauthorized commands issued to control equipment, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), causing an environmental incident, or even disabling control equipment</td>
</tr>
<tr>
<td>Spoofed System Status Information</td>
<td>False information sent to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators</td>
</tr>
<tr>
<td>Control Logic Manipulation</td>
<td>Control system software or configuration settings modified, producing unpredictable results</td>
</tr>
<tr>
<td>Safety Systems Modified</td>
<td>Safety systems operation are manipulated such that they either (1) do not operate when needed or (2) perform incorrect control actions that damage the ICS</td>
</tr>
<tr>
<td>Malware on Control Systems</td>
<td>Malicious software (e.g., virus, worm, Trojan horse) introduced into the system.</td>
</tr>
</tbody>
</table>
Attacks

• Stuxnet
• Sandworm
• TRITON
• CrashOverride
• COSMICENERGY
• PIPEDREAM
• and others
HOW STUXNET WORKED

1. **infection**
   Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. **search**
   Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. **update**
   If the system isn’t a target, Stuxnet does nothing. If it is, the worm attempts to access the Internet and download a more recent version of itself.

4. **compromise**
   The worm then compromises the target system’s logic controllers, exploiting “zero day” vulnerabilities—software weaknesses that haven’t been identified by security experts.

5. **control**
   In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. **deceive and destroy**
   Meanwhile, it provides false feedback to outside controllers, ensuring that they won’t know what’s going wrong until it’s too late to do anything about it.

- USB stick
- Siemens control system
- Attacks logic controllers
- Makes centrifuges spin out of control to failure
Sandworm

• ...hacking unit known widely as “Sandworm,” a group in the Russian Main Intelligence Directorate, or GRU...

• ...BlackEnergy for access and reconnaissance, then KillDisk for destruction...

• BlackEnergy, its first version shortened as BE1, started as a crimeware being sold in the Russian cyber underground as early as 2007. Initially, it was designed as a toolkit for creating botnets for conducting DDoS attacks

• On 23 December 2015, attackers behind the BlackEnergy malware successfully caused power outages for several hours in different regions of Ukraine.
TRITON

• Triton is malware first discovered at a Saudi Arabian petrochemical plant in 2017. It can disable safety instrumented systems, which can then contribute to a plant disaster.

• In December 2017, it was reported that the safety systems of an unidentified power station, believed to be in Saudi Arabia, were compromised when the Triconex industrial safety technology made by Schneider Electric SE was targeted in what is believed to have been a state sponsored attack. The computer security company Symantec claimed that the malware, known as "Triton", exploited a vulnerability in computers running the Microsoft Windows operating system.

• In 2018, FireEye, a company that researches cyber-security, reported that the malware most likely came from the Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM), a research entity in Russia.

https://en.wikipedia.org/wiki/Triton_(malware)
CrashOverride

- The U.S. Government attributes this activity to Russian nation-state cyber actors and assess that Russian nation-state cyber actors deployed CrashOverride malware to conduct a cyberattack against Ukrainian critical infrastructure.
- The modules and capabilities publicly reported appear to focus on organizations using ICS protocols IEC101, IEC104, and IEC61850, which are more commonly used outside the United States in electric power control systems.
- Issues valid commands directly to remote terminal units (RTUs) over ICS protocols. (…and more)
PIPEDREAM

- ... is a **modular ICS attack framework** that an adversary could leverage to cause disruption, degradation, and possibly even destruction depending on targets and the environment.

- ... can manipulate a wide variety of industrial control programmable logic controllers (PLC) and industrial software, including Omron and Schneider Electric controllers, and can attack ubiquitous industrial technologies including CODESYS, Modbus, and Open Platform Communications Unified Architecture (OPC UA).

- ...components...to **enumerate** an industrial environment, **infiltrate** engineering workstations, **exploit** process controllers, cross security and process zones, fundamentally **disable** controllers, and **manipulate** executed logic and programming.

• ...designed to disrupt electric power by interacting with IEC 60870-5-104 (IEC-104) standard devices, such as remote terminal units. These devices are commonly used in electric transmission and distribution operations in Europe the Middle East and Asia.

• ...similarities to malware used in previous attacks targeting electricity grids, including the ‘Industroyer’ incident that took down power in Kiev, Ukraine in 2016.

• ...in the Industroyer attack in 2016, believed to have been perpetrated by Russian APT group Sandworm, the malware issued IEC-104 ON/OFF commands to interact with RTUs, and may have made use of an MSSQL server as a conduit system to access OT. This enabled attackers to send remote commands to affect the actuation of power line switches and circuit breakers, thereby causing power disruption.
Flipper Zero is a portable multi-tool for pentesters and geeks in a toy-like body. It loves hacking digital stuff, such as radio protocols, access control systems and more. It’s fully open-source and customizable, so you can extend it in whatever way you like.

https://flipperzero.one
So What Can We Do?
Accounting Controls Example

In accounting, Internal Control is comprised of the policies and procedures adopted by the management of an entity to assist in achieving the following objectives:

(a) Orderly and efficient conduct of business.
(b) Adherence to management policies
(c) Safeguarding of assets
(d) Prevention and detection of fraud and errors
(e) Accuracy and completeness of accounting records
(f) Timely preparation of financial statements
Security Controls

Cybersecurity controls are the processes an organization has in place to protect itself from computer system vulnerabilities and data hacks.

*IT-oriented* examples include:

- Establish and Maintain Detailed Asset Inventory
- Ensure Network Infrastructure is Up-to-Date
- Establish and Maintain a Security Awareness Program
- Establish and Maintain a Secure Application Development Process
ICS/OT Controls

• Fail-safe design
• Physical security
• Logical separation
• Monitoring
• Secure remote access
5 Reasons Why IT Security Tools Don't Work For OT

• Reason 1: OT prioritizes availability over confidentiality
• Reason 2: OT systems run on always-up legacy systems
• Reason 3: IT tools almost always require a connection
• Reason 4: OT systems are highly variable
• Reason 5: OT systems are delicate

IEC 62443 Standards

International Electrotechnical Commission

As opposed to IEC/ISO 27000 for Information Technology
For the security we said we'd hire someone to...

Hold on, that's not the priority. Let's get the project started first, we'll see about that later...

Hey the project is nearly done, we should do a security audit to...

Too late man, we don't have the time or the budget for that

The site's been online for 10 days, and we haven't done any security testing, I'm nervous...

Don't worry, we'll take care of it later...

Later...

DOWN! THE SITE IS DOWN!

WE'VE BEEN HACKED!

How could you let this happen!?
Secure by Design

“Shift Left”
“A few examples of ... cybersecurity deficiencies in the transmitters include lack of device cyber forensics (no ability to determine what has been changed and by whom); lack of cyber logging (no ability for long-term storage of information as data is overwritten); no capability for implementing antivirus software; lack of patching capabilities; and the use of insecure communication protocols, such as FTP, Modbus, and Bluetooth.”

Weiss, Joseph, “Challenges in Federal Facility Control System Cyber Security, Including Level 0 and 1 Devices,” 2023
Supply Chain Security

• How can you be sure that the components used in control systems can be trusted?
Ecosystems

• Business partners
  • Contracts
  • Business associate agreements
  • Service level agreements
  • Monitoring
  • Auditing
ICS Incident Response Jump Bag

- Laptops with Security Onion, REMnux, SIFT, or RELICS from SANS ICS515
- Approved digital camera (no photo metadata)
- CD-ROM drives and discs
- Hardcopy ICS-specific incident response playbooks and network diagrams
- Network/convertor cables, (e.g., USB to serial)
- Contact list for safety, engineering, integrators, security, and emergency response team
- Forensically clean USBs and external drives
- Log, packet analysis, and timeline tools
- Hashes of field device logic/configuration files
- Baseline images of critical ICS assets
- Data acquisition tools – prioritize command-line tools and memory
- Personal protective equipment (PPE) for safety
- Out-of-band communications, (e.g., handheld radios on-site)
- Site-specific physical safety training certificates
- Offline malware analysis tools (static, interactive, automated)

https://www.sans.org/mlp/ics-resources/?msc=ics%20Field%20Manual%20V3#download-volume3
Hackers only need to get it right once...

...we need to get it right every time
Selected References

• **NIST guidance**
  • Guide to Industrial Control Systems (ICS) Security
    • [https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf)
  • Special Publication NIST SP 800-82r3 ipd, Guide to Operational Technology (OT) Security, Initial Public Draft
  • Securing the Industrial Internet of Things: Cybersecurity for Distributed Energy Resources

• **CISA guidance**
  • Securing Industrial Control systems: A Unified Initiative
  • Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and –Default
    • [https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf](https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf)
Selected References (continued)

• **SANS guidance**
  - ICS Cybersecurity Field Manual series
    - [https://www.sans.org/mlp/ics-resources/](https://www.sans.org/mlp/ics-resources/)

• “Challenges in Federal Facility Control System Cyber Security, Including Level 0 and 1 Devices,” Joseph Weiss, PE, CISM, CRISC Managing Partner, Applied Control Solutions, LLC


42TEK, LLC

Program management & product development for

- data security
- healthcare systems
- critical infrastructure

David Snyder, MBA, PE, CISSP, CCSP

www.42tek.com  david@42tek.com