Jacobs Challenging today. Reinventing tomorrow.

Cybersecurity – Protecting Water System Functionality

Alabama Department of Environmental Management

Drinking Water Branch

27th Annual Surface Water Meeting

Wetumpka, AL

October 14, 2026

Biographies



Benjamin (Ben) Stirling
Director **Cybersecurity & Operational Technology**

Ben has over 20 years of experience in the Power, Oil & Gas, and Industrial sectors. As a thought leader in securing industrial environments, Ben works with end users and OEMs to develop technology stacks and secure architectures. He has a passion for control systems and securing the world's infrastructure combined with deep knowledge of NERC CIP, NIST, ITIL, ISA 99/IEC 62443, and MITRE ATT&CK for ICS. He has a long-established track record of working with industry to recognize and ameliorate cybersecurity risks to infrastructure and human safety.



Gregg Gray, PE
Senior I&C Engineer

Gregg has over 30 years of experience in the Municipal Water and Wastewater industry. At Jacobs, he is responsible for I&C/OT design activities for projects throughout the Southeast. In this role, Gregg develops hardware and software standards for SCADA/OT master plans, control system upgrades, develops network design drawings and specifications, and provides services during construction to ensure that project implementation meets the client's needs.

Increase of Cyber Attacks in Critical Infrastructure

Selected incidents and operational impacts | 2010–2026

Selected Events



Recent Operational Incidents

MAY 2021

COLONIAL PIPELINE

Ransomware forced the operator to halt pipeline operations. The disruption showed how an IT incident can affect fuel delivery and operational continuity.

APRIL 2022

PIPEDREAM

ICS-focused malware was designed to target industrial control systems and could affect multiple vendors' equipment.

FEBRUARY 2023

U.S. ENERGY COMPANY

Adversaries accessed an energy company's OT network. The incident underscored the need to detect and contain access across IT/OT boundaries.

SEPTEMBER 2024

LEBANON DEVICE EXPLOSIONS

Exploding pagers and two-way radios caused mass casualties. The incident highlighted physical and cyber supply-chain risks in electronic devices.

JULY 2026

WATER UTILITIES | AT LEAST 7 STATES

The FBI reported attacks on internet-exposed PLCs at water and wastewater utilities in at least seven states. Actors changed device IP addresses and passwords, disrupting monitoring and control; reported effects included pressure loss and flooding.

2026 source: FBI/EPA Public Service Announcement, July 30, 2026. At least seven states; reported impacts included loss of monitoring/control, pressure loss and flooding.

Recent Cyber Activity Targeting Water and Critical Infrastructure

100+ water utilities affected – One of the most widespread cyber campaigns in U.S. water sector history



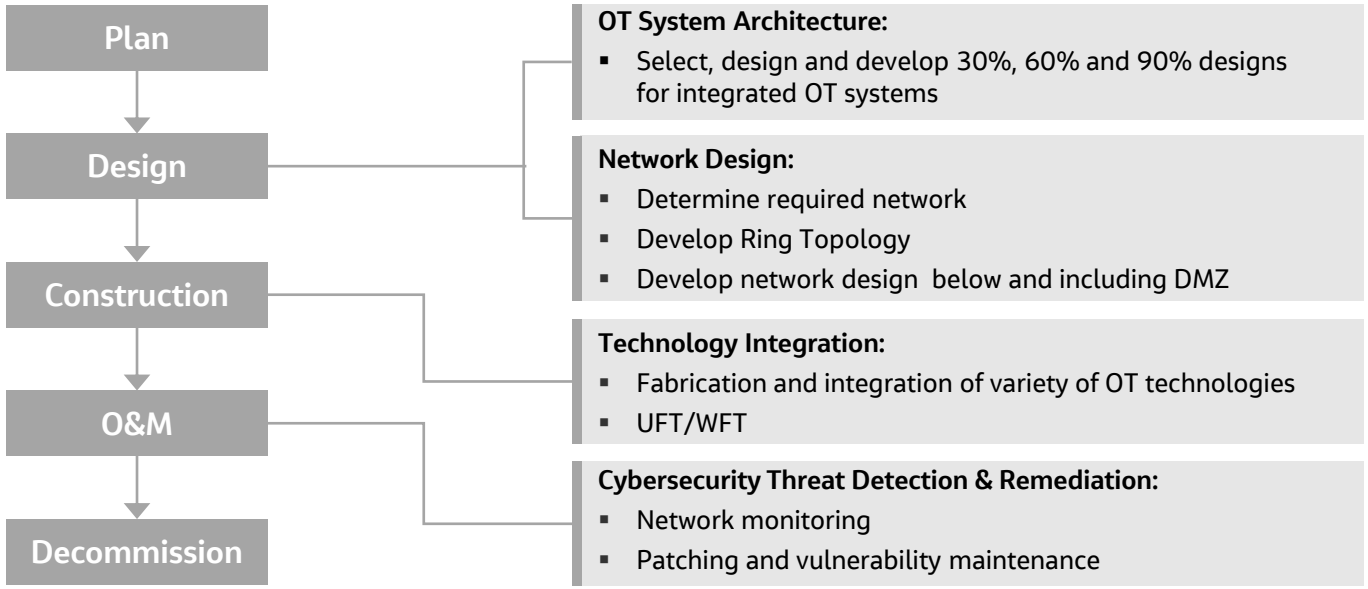
Part of a nationwide cyber campaign targeting water utilities and critical infrastructure – not an isolated incident.

©Jacobs 2026

Jacobs' Business Overview

Jacobs is the market leader in water sector OT cybersecurity

OT Cyber Team Delivers Throughout Jacobs Delivery Lifecycle



- 40 unique water utility sites served with OT cybersecurity in FY2024
- 30 cybersecurity assessments
- 10+ active projects in design and integration of control systems & OT
- 20+ water utility sites served with O&M cybersecurity services including managed services
- Major wastewater OT cybersecurity projects in Wilmington and Clark Regional Wastewater

45,000 employees

Serve 6 markets in geographies around the world

Global leader in water sector

5,000 employees in US water sector/9,000 employes in water sector globally

Unrivaled bench strength in water sector OT cybersecurity and I&C personnel

©Jacobs 2026

First Client Case Study: Incident timeline and operating impact

July 2026 · 1 a.m.

Communications lost to ten (10) remote water sites.

By itself, not that uncommon – cellular provider occasionally exhibits brief loss of service.

The normal response – reboot the cellular modems – did not resolve the issue.

Client noticed equipment shutting down and system pressures dropping.

Under attack: Key signals at plants and other sites indicated a much bigger problem.

©Jacobs 2026

Client Responses

Visit each remote site

PLC processors were no longer in Run mode.

PLC IP addresses had been changed.

PLCs had new passwords established.

Clear PLC

Client wiped PLC processor memory by pulling both power and battery.

Reload PLC program

Client had relatively recent backups on hand.

Client performs backups of telemetry PLC programs twice per year with time change.

Backups sufficient as limited changes are made to telemetry PLC programs.

Seek 3rd Party Assistance

Client contacted Jacobs first thing the next morning.

Client engaged third-party to perform systemwide audit.

©Jacobs 2026

Response, recovery and Jacobs' role

Suspect Activity

Jacobs was able to respond quickly and had suspicions that this was a cyber incident.

Jacobs contacted other clients who indicated similar issues commencing around the same time.

Client Assistance

Jacobs immediately advised the Client to place all PLC keyswitches to RUN (not REMOTE-RUN).

Jacobs assisted in the Client's investigation process by gathering system data and log files to support the third-party audit team.

Jacobs flashed/updated PLC firmware to ensure clean install using latest manufacturer updates.

Also flashed/updated cellular modem firmware.

Private APN Migration

Transitioned all telemetry sites to Private APN. Trained Client on how to do this to "divide-and-conquer" all sites in a timely manner.

APN = Access Point Name

Private APNs are established by cellular providers to implement gateways to keep traffic off of the public internet.

©Jacobs 2026

Second Client Case Study: Incident timeline and operating impact

Also July 2026 · 1 a.m.

Communications lost to twelve (12) remote water sites.

Client assumed the issue was with the cellular provider. Again, not that uncommon for brief outages.

Client performed hourly in-person inspections of affected sites, checking tank levels and manually operating pumps, as needed.

Client completely unaware the situation was the result of a cybersecurity attack and continued to assume a provider outage.

©Jacobs 2026

Response, recovery and Jacobs' role

Proactive Check-In

Jacobs contacted the Client based on (a) knowledge that this was a bigger situation and (b) previous knowledge of the Client's architecture.

Upon understanding cause, the Client requested immediate assistance.

Client Assistance

Flashed/updated PLC firmware.

Flashed/updated cellular modem firmware.

Reloaded PLC programs from backups.

Placed all PLC keyswitches in RUN mode.

Worked with cellular provider to migrate the Client's remote sites to a Private APN network.

Why Targeted?

In both case studies, the Client's equipment was fully accessible from the public internet.

PLC keyswitches were in the Remote position allowing programming software to remotely change the mode of the processor.

PLCs had no or weak passwords.

©Jacobs 2026

Minimize Exposure of Assets to the Public Facing Internet

Private APN

As previously mentioned, this is one method of removing PLCs from public internet access.

Why not already implemented as such?

- There are setup and maintenance costs for the service from the cellular provider.
- Any routing changes must involve the cellular company.
- The threat landscape has changed in recent years.

SD WAN

SD WAN = Software-Defined Wide Area Network

This is a virtualized network technology that uses software to manage, control, and optimize network traffic over WAN connections such as cellular and fiber networks.

It is independent of the underlying physical infrastructure.

Builds encrypted VPN tunnels across public or mixed connections.

IPSec Tunnels

Some existing implementations may use IPSec for building secure VPN tunnels or routes.

IPSec is a secure encryption protocol but can be cumbersome to implement and especially to maintain. Many firewall providers are phasing out support of IPSec tunnels.

SD WAN is an emerging technology and provides more resiliency than IPSec VPNs.

However, these type of solutions require IT/OT configuration effort, whether by the Client or an OT vendor.

The Client should consider their options based upon their specific needs and resources.

©Jacobs 2026

Third Client Case Study: Incident timeline and operating impact

Jan 18 · 1 p.m.

A ransomware note is created in the affected environment.

Jan 19

Client IT discovers the incident; IT and SCADA networks both compromised. Control network is operated manually.

Response phase

Specialists handle forensic review, log analysis, and restoration work.

Jan 23

Recovery support team is onsite.

Operating mode

The utility ran the control network manually while response teams investigated the incident and planned restoration.

©Jacobs 2026

Attack path and security gaps

Identity entry

Unpatched edge SCADA Firewall breached. Password spraying targeted weak, aging, and re-used credentials.

Account foothold

A new account appeared, enabling broader movement through SCADA domain services.

Boundary bypass

An unlabeled cable was discovered that connected business and control networks, bypassing intended separation.

Recovery impaired

Movement reached all SCADA and IT administrative systems. Backups were stopped or deleted before encryption.

©Jacobs 2026

Response, recovery and Jacobs' role

Maintain safe operations

The control network operated manually while the response team assessed the affected environment. Teams preserved forensic evidence and logs as they investigated scope and prepared recovery.

Restore in a controlled sequence

Restore domain controllers and validate virtualization recovery data. Rotate credentials and review suspicious accounts. Rebuild firewalls, tighten segmentation, remove temporary access, and validate systems before reconnecting.

Jacobs' role

Jacobs supported the investigation and restoration effort. We helped restore affected systems and strengthen system and network controls as the environment was rebuilt.

©Jacobs 2026

Best practices and Jacobs support

Utility practices informed by this incident

Verify the actual boundary

Inventory, trace, and label every cable and remote path. Test separation between business and OT systems after changes.

Harden identity and remote access

Require MFA and unique credentials. Remove stale accounts and alert on password spraying or new account creation.

Isolate recovery assets

Keep immutable or offline backups outside daily admin paths. Test restores for identity, virtualization, firewall, and control configurations.

Practice safe restoration

Plan manual operations, evidence preservation, and staged reconnection. Validate integrity before systems return to service.

How Jacobs can help

- Field-verify OT assets, cabling, and network paths.
- Assess identity, remote access, and segmentation.
- Plan OT response, manual operations, and recovery.
- Exercise the plan with operations, IT, and security teams.

©Jacobs 2026

What's Wrong with this picture (It’s not just the Water Sector)

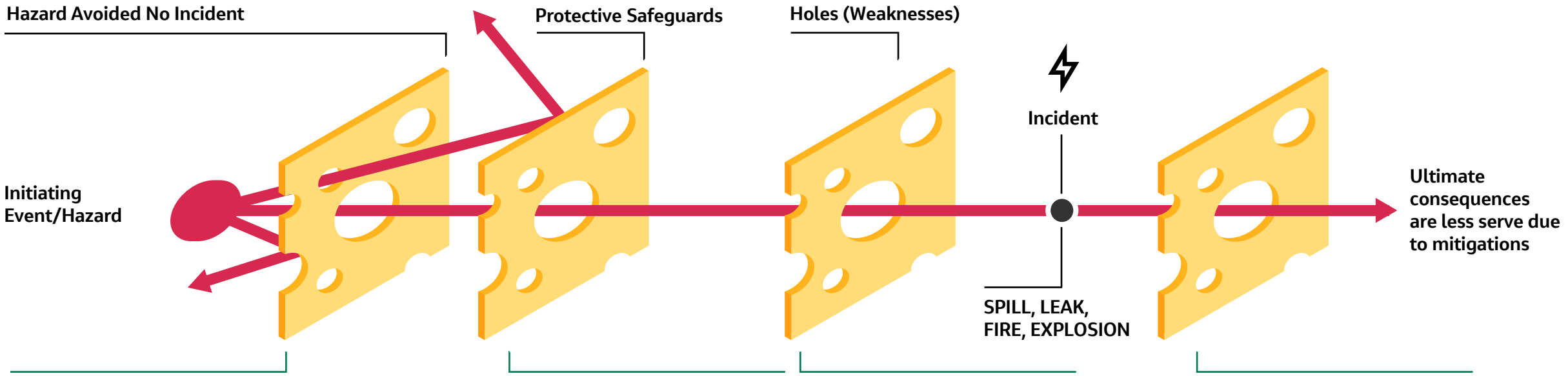




©Jacobs 2026

When Risks Align

Expect the unexpected. Assess your risks. Prevent Incidents.



Engineering Controls
- Design or architecture
- Monitoring of controls networks and DMZs
- Isolation of risks and reduction of attach surfaces

Administrative Controls
- Supply chain security controls
- Adoption of risk-based cybersecurity framework
- Management of change

Behavioral Controls
- Use of least privilege access (RBAC)
- Use of effective cybersecurity controls
- Use training of operators and plant personnel
- Assessmentss, tabletops, and continuous improvement

Post-incident Mitigation
- Specific incident response plan
- Recovery and restoration
- Root cause analysis

Learn More: https://www.mtu.edu/chemical/facilities/safety/?utm_campaign=MTU+Recruitment&utm_source=vanity&utm_medium=referral&utm_content=/process-safety

©Jacobs 2026

Start with the SANS ICS 5 Critical Controls



SCADA Incident Response Plan



Defensible Architecture



SCADA Network Visibility and Monitoring



Secure Remote Access



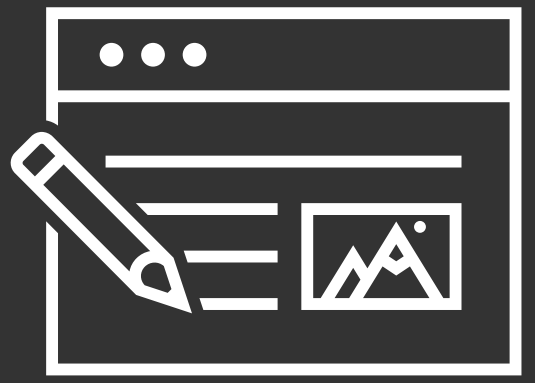
Risk-Based Vulnerability Management

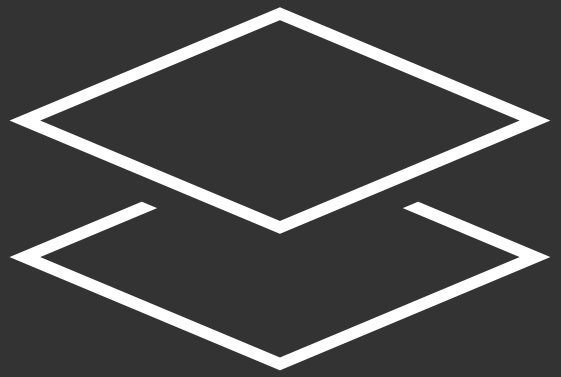
Note: that the order of the controls is the recommended order of implementation

The SANS 5 Critical Controls

ICS Incident Response Plan

You should create a detailed incident response plan specifically tailored for your SCADA environment(s). This plan should cover procedures for detecting, responding to, and recovering from incidents including disaster recovery. It must outline clear roles and responsibilities, communication protocols, and steps for containing and recovering from incidents.





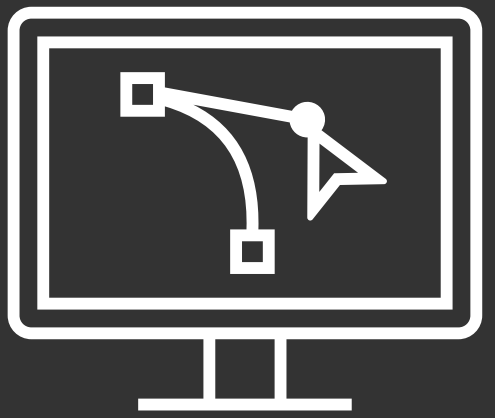
Defensible Architecture

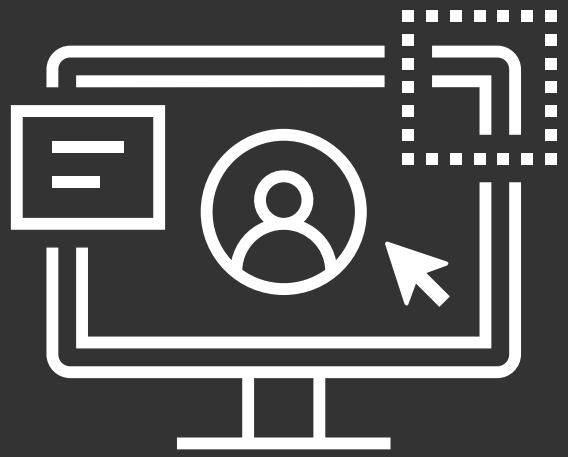
Design a network architecture that efficiently segments and isolates critical systems. The aim is to minimize the attack surface and mitigate the impact of incidents. Implement network segmentation that: enforce stringent access controls and use demilitarized zones (DMZs) to separate industrial networks from IT / Business networks.

The SANS 5 Critical Controls

SCADA Network Visibility and Monitoring

Implement a continuous monitoring strategy of SCADA networks to swiftly detect anomalies and potential threats. Utilize specialized monitoring tools and technologies that offer deep visibility into network traffic and system activities, ensuring that anomalies and threats are quickly identified and addressed.





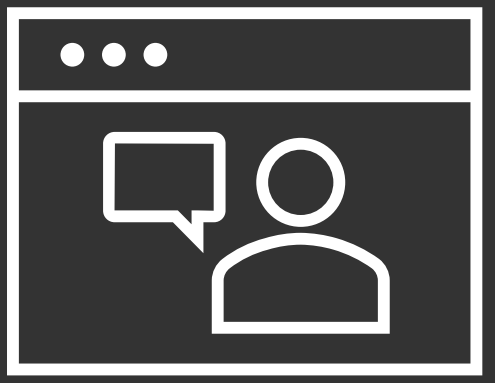
Secure Remote Access

Deploy a secure remote access solutions to efficiently manage and monitor access to SCADA environments. If possible, use multi-factor authentication, encryption, and enforce stringent access controls to ensure remote access is both secure and compliant with organizational policies.

The SANS 5 Critical Controls

Risk-Based Vulnerability Management

Perform systematic vulnerability assessments and prioritize remediation efforts based on the potential impact and exposure of critical systems. Identify, evaluate, and address vulnerabilities within SCADA components, concentrating on those that pose the highest risk to the organization's critical assets and operations.



Creating a risk-based supply chain vulnerability management plan. **Scope:** Define the scope, including the systems, processes, and stakeholders involved. **Supply Chain Mapping:** Document all suppliers, and the critical components they provide. **Threat Analysis:** Identify potential threats: cyber-attacks, natural disasters, geopolitical issues, and supplier failures. Evaluate the vulnerabilities within your supply chain. **Impact Analysis:** Assess the potential impact of identified risks on your operations, financials, and reputation. Determine the probability of each risk occurring. **Risk Prioritization:** Rank risks based on their impact and likelihood to focus on the most critical vulnerabilities.

©Jacobs 2026

Jacobs Joins Dragos Community Defense Program



- OT specific IR
- Consulting and implementation of Defeasible Architecture
- Dragos Platform implementation
- Secure remote access (announcement Coming)
- Risk based Maintenance and vulnerability management

https://www.jacobs.com/newsroom/news/jacobs-and-dragos-collaborate-strengthen-cybersecurity-vulnerable-us-water-facilities

©Jacobs 2026

What Now?

Are your Safety, Cybersecurity, and Operations teams prepared?

Be proactive

- Start now - Incorporate cybersecurity into current management procedures
- Help mangers gain understanding of existing system
- Identify equipment and assets that could be targeted in a cybersecurity incident
- Consider upgrading obsolete equipment and assets
- Enhance organizational awareness of external connections
- Develop OT/ICS/SCADA specific plans (both inventory & incident response plans)
- Implement and validate regularly-scheduled backups of all programming and configurations (PLC, HMI/SCADA, switches, firewalls, etc.)
- Change default passwords on network equipment and enable passwords for PLCs.
- Seek EPA guidance outlining response strategies

©Jacobs 2026

Questions or Comments?

Thank you!

Jacobs

Challenging today.
Reinventing tomorrow.

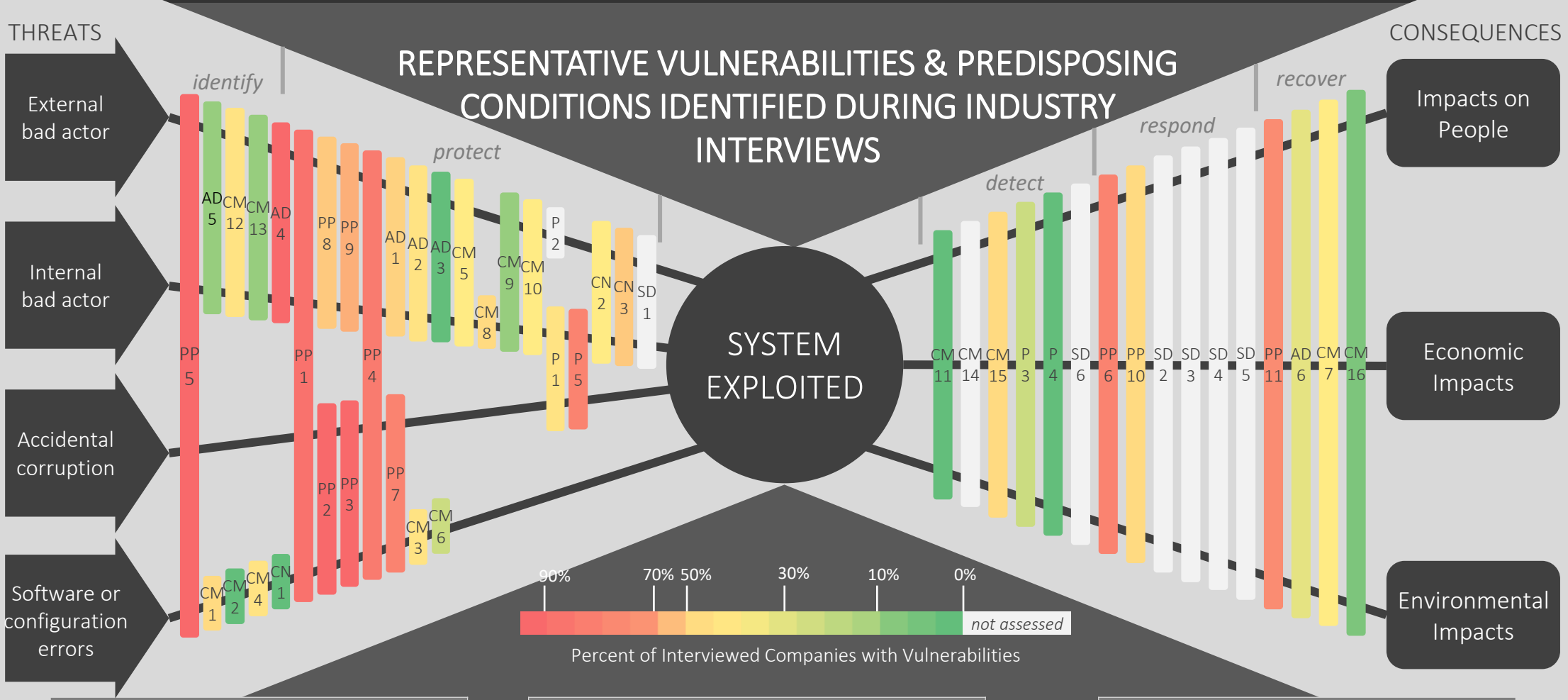
Appendix

Resources

- Alabama State and Local Cybersecurity Grant Program https://slcgp.alabama.gov/
- EPA, Cybersecurity for the Water Sector https://www.epa.gov/cyberwater
- FBI Cyber Alerts https://www.fbi.gov/investigate/cyber/alerts
- Cybersecurity Supply Chain Risk Management: Fact Sheet (nist.gov)
- ICT Supply Chain Resource Library | CISA
- Empowering SMBs: A Resource Guide For Developing A Resilient Supply Chain Risk Management Plan (cisa.gov)
- NERC CIP-013-01 - Standard (nerc.com)

©Jacobs 2026

REPRESENTATIVE VULNERABILITIES & PREDISPOSING CONDITIONS IDENTIFIED DURING INDUSTRY INTERVIEWS



POLICY & PROCEDURE (PP)	
PP 1	Inadequate security policy for the ICS
PP 2	No formal ICS security training and awareness program
PP 3	Absent or deficient ICS equipment implementation guidelines
PP 4	Lack of administrative mechanisms for security policy enforcement
PP 5	Inadequate review of the effectiveness of the ICS security controls
PP 6	No ICS-specific contingency plan
PP 7	Lack of configuration management policy
PP 8	Lack of adequate access control policy
PP 9	Lack of adequate authentication policy
PP 10	Inadequate incident detection and response plan and procedures
PP 11	Lack of redundancy in critical components (single point of failure)
ARCHITECTURE & DESIGN (AD)	
AD 1	Inadequate incorporation of security into architecture and design.
AD 2	Insecure architecture allowed to evolve
AD 3	No security perimeter defined
AD 4	Control networks used for non- control traffic
AD 5	Control network services not within the control network
AD 6	Inadequate collection of event data history

CONFIGURATION & MAINTENANCE (CM)	
CM 1	Hardware, firmware, and software not under configuration management.
CM 2	OS/vendor software patches developed significantly after vulnerabilities found
CM 3	OS/application security patches not maintained or vendor declines to patch
CM 4	Inadequate testing of security changes
CM 5	Poor remote access controls
CM 6	Poor configurations are used
CM 7	Critical configurations are not stored or backed up
CM 8	Data unprotected on portable device
CM 9	Passwords generation, use, and protection not in accord with policy
CM 10	Inadequate access controls applied
CM 11	Improper data linking
CM 12	Malware protection not installed or up to date
CM 13	Malware protection implemented without sufficient testing
CM 14	Denial of service (DoS)
CM 15	Intrusion detection/prevention software not installed
CM 16	Logs not maintained

PHYSICAL (P)	
P 1	Unauthorized personnel have physical access to equipment
P 2	Radio frequency and electro- magnetic pulse (EMP)
P 3	Lack of backup power
P 4	Loss of environmental control
P 5	Unsecured physical ports
COMMUNICATION & NETWORK CONFIGURATION (CN)	
CN 1	Improper Data Validation
CN 2	Installed security capabilities not enabled by default
CN 3	Inadequate authentication, privileges, and access control in software
SOFTWARE DEVELOPMENT (SD)	
SD 1	Denial of Control Action
SD 2	Control Devices Reprogrammed
SD 3	Spoofed System Status Information
SD 4	Control Logic Manipulation
SD 5	Safety Systems Modified
SD 6	Malware on Control Systems

INITIAL ACCESS	EXECUTION	PERSISTENCE	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network ConnectionEnumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/ Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings		Manipulation of View
						Screen Capture		Modify Control Logic		Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Approaching Cybersecurity in a Converged Environment

- Secure-by-Design -> Consequence-based, Cyber-informed Engineering (CCE) and OT Cyber Risk Management
- Business enabler, not a cost center
- Zero-Trust Architecture (ZTA)/ZTNA

CCE PROCESS

PHASE 1 Consequence Prioritization	PHASE 2 System-of- Systems Analysis	PHASE 3 Consequence- Based Targeting	PHASE 4 Mitigations and Protections
Focus on the risk management framework to identify critical operations that must remain functional and evaluate the associated attack scenarios that could disrupt them.	Collect information to map the interdependencies and pathways between critical processes, defense systems, and components.	Determine the adversary's path to achieve the highest impact effects and what information is required to achieve those goals.	Eliminate or disrupt digital attack paths to the greatest extent possible.

Supply Chain Risk Management: A Cybersecurity Perspective

Definition: Identifying, assessing, and mitigating risks within the supply chain to ensure the integrity, security, and resilience of products and services (before they get to the plant).

Key Cybersecurity Risks

- **Third-Party Vendors**: Risks from suppliers and service providers.
- **Breaches**: Unauthorized access to sensitive information, manufacturing, or equipment.
- **Malware and Ransomware**: Cyberattacks targeting supply chain components or facilities.

Best Practices

- **Risk Assessment**: establish a cadence to evaluate suppliers' cybersecurity measures and risk profile.
- **Transparency:** Improve visibility into the supply chain.
- **Compliance:** Ensure adherence to cybersecurity standards and regulations.

Case Studies

- **NIST Guidelines:** Implementation of NIST's Cybersecurity Supply Chain Risk Management Practices.
- **Real-World Examples:**

SolarWinds Orion, Kaseya VSA, NotPetya, MOVEit Transfer

Conclusion

- **Proactive Measures:** Current events and prudence; emphasize the need for continuous monitoring and improvement of cybersecurity practices within the supply chain.

Jacobs Supply Chain & Procurement

Increase scrutiny	Vendor questionnaire and interview process
	Ensure compliance with SOC2 and other standards
	Stringent validation vs simple compliance of security frameworks
SBOM	Reviewing any use of open-source code for vulnerabilities
	Critical technology software and firmware
	Imperative to identify and manage risks with transparency components
Standards	ISA99/IEC62443
	NIST 800-161
	NERC CIP-013-1
	AWIA 2018 / AWWA Standards (Evolving)

©Jacobs 2026

Copyright notice

Important

© Copyright Jacobs Group 2026 . All rights reserved. The content and information contained in this presentation are the property of the Jacobs Group of companies (“Jacobs Group”). Publication, distribution, or reproduction of this presentation in whole or in part without the written permission of Jacobs Group constitutes an infringement of copyright. Jacobs, the Jacobs logo, and all other Jacobs Group trademarks are the property of Jacobs Group.

NOTICE: This presentation has been prepared exclusively for the use and benefit of Jacobs Group client. Jacobs Group accepts no liability or responsibility for any use or reliance upon this presentation by any third party.

©Jacobs 2026