DPAS

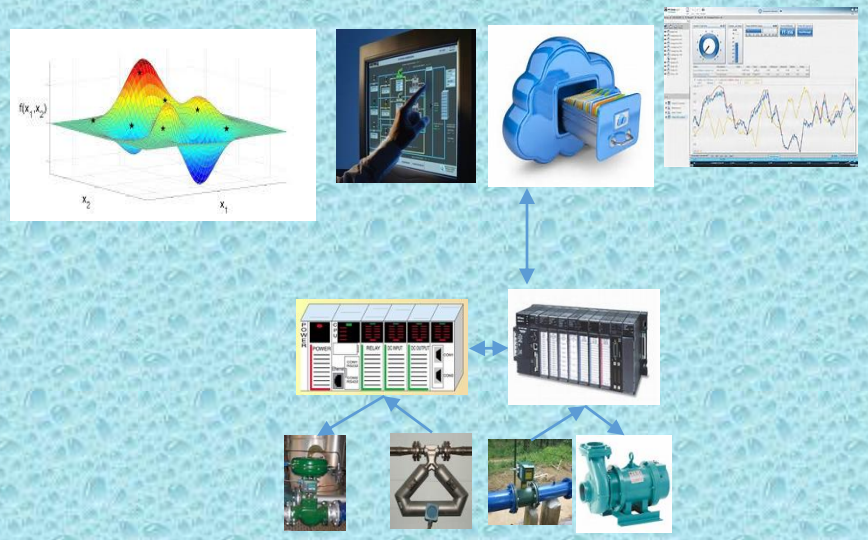
WaterTight

Protecting operations and data

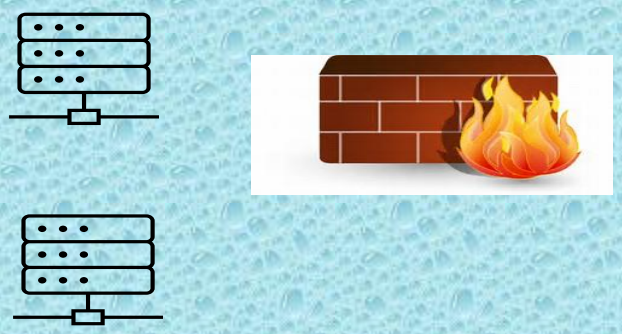
Cyber security for SCADA

Let us perform an audit to find your vulnerabilities

Operational Technology



Information Technology



DPAS

Compliance

Examples of requirements that apply to municipal water systems

AWIA Section 2013/SDWA Section 1433: Risk and Resilience Assessments and Emergency Response Plans

On October 23, 2018, America's Water Infrastructure Act (AWIA) was signed into law. AWIA section 2013, which amended section 1433 of the Safe Drinking Water Act (SDWA), requires community (drinking) water systems (CWSs) serving more than 3,300 people to develop or update risk and resilience assessments (RRAs) and emergency response plans (ERPs). The law specifies the components that the RRAs and ERPs must address, and establishes deadlines by which water systems must certify to EPA completion of the RRA and ERP. The Federal Register Notice for New Risk Assessments and Emergency Response Plans for Community Water Systems is available.

SDWA section 1433 also states that EPA should provide guidance and technical assistance to water systems that serve less than 3,301 people on how to conduct RRAs and ERPs, though these systems are not required to certify completion to EPA.

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

RELATED TOPICS: CYBERSECURITY BEST PRACTICES, CYBER THREATS AND ADVISORIES

REPORT A CYBER ISSUE Organizations should report anomalous cyber activity and/or cyber incidents 24/7 to report@cisa.gov or 1-844-Say-CISA.

In March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Enactment of CIRCIA marked an important milestone in improving America's cybersecurity by, among other things, requiring the Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA. These reports will allow CISA to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims.

ERP Requirements and Assistance Resource for CWSs that Serve More than 3,300

No later than six months after certifying completion of its RRA, each system must prepare or revise, where necessary, an ERP that incorporates the findings of the RRA. The ERP shall include:

1. strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system;
2. plans and procedures that can be implemented, and identification of equipment that can be utilized, in the event of a malevolent act or natural hazard that threatens the ability of the community water system to deliver safe drinking water;
3. actions, procedures and equipment which can obviate or significantly lessen the impact of a malevolent act or natural hazard on the public health and the safety and supply of drinking water provided to communities and individuals, including the development of alternative source water options, relocation of water intakes and construction of flood protection barriers; and
4. strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system.

Community water systems shall to the extent possible coordinate with local emergency planning committees established under the Emergency Planning and Community Right-To-Know Act of 1986 when preparing or revising an RRA or ERP under SDWA section 1433. Further, systems must maintain a copy of the RRA and ERP for five years after certifying the plan to the EPA.

https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

https://www.epa.gov/waterresilience/awia-section-2013#ERP

DPAS

Threats: SCADA systems are vulnerable

60 Minutes – Newsmakers

China is hacking America's critical infrastructure, former NSA and retired Gen. Tim Haugh warns

By Scott Pelley

October 12, 2025 / 7:30 PM EDT / CBS News

https://www.cbsnews.com/news/china-hacking-us-critical-infrastructure-retired-general-tim-haugh-warns-60-minutes-transcript/

"If you are willing to go after a small water provider in Littleton, Massachusetts, what other target is off the list?"

Cybersecurity and Cyber Risk Management

Cyber events continue to be identified as a significant risk due to the increasing use of and reliance on technology systems including process control systems, industrial internet, cloud services, and other connected technology. As a result, the sector has experienced a related increase in cyber threats, cyber vulnerabilities, and capabilities of malicious actors. This Roadmap emphasizes the importance of established technology systems while also recognizing that the adoption of new technologies (e.g., Artificial Intelligence (AI)) represents both benefits and increasing challenges to the sector.

"Roadmap to a Secure and Resilient Water and Wastewater Sector", EPA 810-R-24-002

Hackers target Arkansas City water treatment plant, prompting federal investigation

SEPTEMBER 24, 2024

https://industrialcyber.co/utilities-energy-power-water-waste/hackers-target-arkansas-city-water-treatment-plant-prompting-federal-investigation/

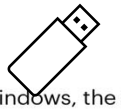
WestRock Ransomware Attack: A Timeline

On **January 25th, 2021**, WestRock, the second-largest packaging company in the United States, **announced** that it has been the victim of a ransomware attack.

The WestRock ransomware attack impacted some of the company's core operational technology (OT) systems and hindered production and packaging-converting operations, which resulted in lagged production levels.

https://heimdalsecurity.com/blog/westrock-ransomware-attack/

How did Stuxnet work?



Stuxnet attacks all layers of its target infrastructure: Windows, the Siemens software running on windows that controls the PLCs, and the embedded software on the PLCs themselves. It is designed to be delivered via a removable drive like a USB stick—the Natanz facility where the uranium enrichment was taking place was known to be *air-gapped,* with its systems not connected to the internet—but also to spread quickly and indiscriminately from machine to machine on an internal network.

https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

Triton (malware)

5 languages

Article Talk | Read Edit View history Tools

From Wikipedia, the free encyclopedia

Triton is malware first discovered at a Saudi Arabian petrochemical plant in 2017.[1][2] It can disable safety instrumented systems, which can then contribute to a plant disaster.[3]

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.[2]

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.[4]

It was reported by Wired that Triton's attacks were registered in North America, China, and Russia.[5]

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

DPAS

Water Sector Lead Cyber Consultant

Steve Mustard

https://www.linkedin.com/in/steve-mustard-794a0a2/

Steve Mustard is an industrial automation consultant with more than 35 years of engineering experience across multiple sectors. He is a licensed Professional Engineer (PE) in Texas and Kansas, a Liveryman of the Worshipful Company of Engineers, an ISA Certified Automation Professional® (CAP®), a UK registered Chartered Engineer (CEng), a European registered Engineer (Eur Ing), a GIAC Global Industrial Cyber Security Professional (GICSP), and a Certified Mission Critical Professional (CMCP).

He was the 2021 President of the International Society of Automation (ISA) and is a Life Fellow of the Society. He is a Fellow of the Institution of Engineering and Technology, and a member of the Water Environment Federation (WEF) Safety and Security Committee.

Mustard writes and presents on a wide array of technical topics and is the author of "Industrial Cybersecurity, Case Studies and Best Practices" and 'Mission Critical Operations Primer", both published by ISA, and "A Guide to Cybersecurity for Water and Wastewater Utilities", published by WEF. He has also contributed to other technical books, including "Project Management: A Technician's Guide", published by ISA, WEF's "Design of Water Resource Recovery Facilities, Manual of Practice No.8, Sixth Edition", and "The Digital Twin", published by Springer Nature.

Mustard's previous and current client list includes: the UK Ministry of Defence; NATO; major utilities, such as Anglian Water Services and Sydney Water Corporation; major oil and gas companies, such as bp, BG Group and Shell; Fortune 500 companies, such as Quintiles Laboratories; and other leading organizations.

DPAS

OT/SCADA Experience

Pat Dixon, PE, PMP

President, DPAS (www.DPAS-INC.com)

Professional engineer TX, WA, VA, CO

Began career in industrial control systems in 1984, experience on several SCADA and DCS platforms, Ignition Gold certified

Project manager for SCADA and cyber security for 2 water treatment facilities for International Border Water Commission

Served 2 terms on Lago Vista TX city council, liaison to Lower Colorado River Authority (LCRA)

https://www.linkedin.com/in/dixonpatrick/

Joseph Burns

Ignition Gold certified

Developer of Flintium, Ignition objects for Rockwell PlantPAX Logix library

Developer of “Pidbot” - Industrial process modeling & PID tuning software.

Experience with Rockwell Studio5000, Wonderware, Ignition, and FactoryTalk.

https://www.linkedin.com/in/joseph-burns-96a899134/

DPAS

IT/OT Experience

Ed Torres

SCADA engineer for building up the SCADA workstation which includes the task of selecting the required hardware for the PC, formatting and setting up of the Operating System and configuration on the network interface card on Windows NT Server/Client OS using TCP/IP

Experienced in networking and domain administration, specialization includes DNS, Active Directory Services

Advanced user on the following Operating Systems: Windows NT, Windows XP, Windows 2003, Windows Vista, Windows 7, Windows 2008 and Hyper-V Server. Well experienced in setting up test systems using Dell computers/server and Cisco routers/firewall.

https://www.linkedin.com/in/edmtorres/

Hugo Parodi

For Pederneles Electric Coop managed the daily operations, installation, and maintenance of enterprise-wide networks for video, voice, wireless, and data

VMware Certified Professional 6 - Network Virtualization (VCP6-NV)

Cisco Certified Network Professional - Route & Switch

Cisco Certified Specialist - Enterprise Core

Cisco Certified Network Associate Routing and Switching

Juniper Networks Certified Associate, Junos (JNCIA-Junos)

https://www.linkedin.com/in/hugo-parodi-779a5321/

DPAS

IT/Cyber Experience

Raj Puchakayala

Professional Cybersecurity Engineer

15+ years experience in IT

AWS, GCP Certified.

Enterprise Architecture, Security Automation, AI, Data Science, Cybersecurity. Observability, Security Monitoring

Lafayette Green

Over 23 years as an Information Security Analyst/Information Technology Specialist for the US Army

Extensive experience planning, coordinating and administering Windows and UNIX servers for system optimization of unclassified and classified Department of Defense networks

Areas of expertise include: Department of Defense (DoD) Information Technology (IT) Acquisition, Information Assurance (IA), DoD IT Certification and Accreditation (C&A) or Assessment and Authorization (A&A), IT (Cyber) Security Risk Analysis & verification, Special Security Representative

https://www.linkedin.com/in/lafayettejgreen/

DPAS

IT/Cyber Experience

Dr Tameka Rose

- Seasoned information security professional with over 20 years of experience.
- Specializes is risk management documentation and security of cloud and legacy infrastructures for federal government systems.
- Supported security of mission essential systems for Department of Homeland Security (DHS), Federal Communication Commissions (FCC), United States Department of Agriculture, (USDA), and Department of Defense (DoD).
- Doctorate from Capella University in Information Technology – Information Assurance and Cybersecurity
- Amazon Web Services Certified Cloud Practitioner (AWS CCP) and Certified Authorization Professional (CAP).

https://www.linkedin.com/in/dr-tameka-rose-9081b4b2/

Donnell Stockton

Cybersecurity professional with 10+ years of experience in Information Assurance (IA) and INFOSEC, supporting the Intelligence Community (IC). Skilled in IT risk management, system Assessment & Authorization (A&A), and cybersecurity risk analysis, with specialized expertise in Department of Justice (DOJ) IT systems and the DOJ Risk Management Framework.

Developed and delivered FISMA/FedRAMP-compliant Security Authorization Packages (SSPs, POA&Ms, IRPs, CM Plans, PIAs) to support successful authorizations.

https://www.linkedin.com/in/donnell-stockton-91ba321/

DPAS

Project Management Experience

Rear Admiral Reginald Hendrix

https://www.linkedin.com/in/reginald-hendrix-rear-admiral-usn-b9750961/

https://www.navy.mil/Leadership/Flag-Officer-Biographies/BioDisplay/Article/3923727/rear-admiral-reginald-hendrix/

Senior level manager with over 25 years of military and private industry experience

Deputy Commander of Navy Expeditionary Combat Command (NECC) responsible for manning, training, equipping, organizing, and sustaining the Navy Expeditionary Combat Force (NECF)

As IT / Cyber Security Project Manager for CACI International, managed the overall coordination of IT projects, from planning through implementation. Directed Network Engineers in all aspects of Cyber-Security network operations.

Responsible for supporting National Geospatial-Intelligence Agency (NGA) program business and functional operations to include identifying and facilitating resolution of operational issues and acting as a liaison between technical and functional areas of CIO staff. Supports the Program Management Office (PMO) in executing, monitoring information technology systems related to national security.

DPAS

Plan

Vulnerability Audit

- Identify risks
- Determine scope of service
- Require access to information and systems
- Since we are a startup, we are offering a low-cost audit service for initial customers for references on our future opportunities
- We can start with the EPA evaluation

EPA's Water Sector Cybersecurity Evaluation Program

DID YOU KNOW: Performing a cybersecurity assessment could reduce the risk of a cyber attack by up to 45%?

Drinking water and wastewater utilities can use this form to request a free cybersecurity assessment. This evaluation will provide the assessed utility with a risk mitigation template to help understand discovered cybersecurity vulnerabilities and provide guidance on enhancing overall cybersecurity posture.

Support contract

- Routine inspection
- Patch management

Fixed price quotes for projects, such as:

- Switch upgrades
- Managed switch configuration
- Virtualization
- USB virus scan
- Network intrusion monitor