Operational Technology (OT) Cybersecurity Compliance with ASSURANT™ Suite

Enhancing Cybersecurity for Municipal Water Treatment Plants with ASSURANT™ Suite

Shawn Reynolds

7/9/25

1 INTRODUCTION

Municipal water treatment plants are at the forefront of operational technology (OT) cybersecurity research, as they represent a critical component of national infrastructure increasingly exposed to cyber threats. Their distributed design and reliance on interconnected OT systems, alongside conventional information technology (IT), make them especially susceptible to attacks. As a result, research efforts are intensifying to safeguard these essential facilities from growing cyber risks.

Recent incidents, including the 2021 unauthorized-access incident at a drinking water facility in Oldsmar, Florida, and the 2024 ransomware incident reported by Arkansas City, Kansas, highlight the vulnerability of water-sector OT environments to cyber threats. These incidents underscore the need for cybersecurity capabilities that extend beyond monitoring and access control to include system modeling, attack-path analysis, vulnerability correlation, risk prioritization, and evidence generation for audits and regulatory reviews.

OT cyber practitioners currently leverage open-source tools, such as Suricata, Sysmon with Winlogbeat, Logstash, Elasticsearch, Kibana, and Apache NiFi, for monitoring logs and network traffic in OT environments. While effective at creating visibility, these tools offer limited proactive cybersecurity capabilities, such as threat modeling, attack-path visualization, and compliance documentation.

The ASSURANT™ Suite from Knowledge Based Systems, Inc. (KBSI) (please visit www.assurantcyber.com) was developed specifically to address the broader cybersecurity needs of OT systems. It addresses existing capability gaps by providing a comprehensive platform for modeling, analyzing, and mitigating cyber risks in cyber-physical systems.

This white paper describes the ASSURANT™ Suite and outlines the use case in which the ASSURANT™ Suite is deployed to enhance cybersecurity resilience in municipal water treatment plants.

2 CYBERSECURITY CHALLENGES IN MUNICIPAL WATER TREATMENT PLANTS

2.1 CHALLENGES OF SECURING OT NETWORKS IN REAL-TIME SYSTEMS

Municipal water treatment plants heavily rely on Operational Technology (OT) networks to oversee critical functions, including water purification, distribution, and wastewater management. These networks, composed of supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), and human-machine interfaces (HMIs), along with the communication networks that interconnect them, form the backbone of continuous and safe operations.

The unique characteristics of OT environments, particularly their real-time operational requirements, introduce significant cybersecurity challenges that differ markedly from those encountered in traditional IT systems.

One of the most prominent techniques for monitoring cyber-enabled systems is the periodic scanning of network elements and traffic to detect emerging vulnerabilities. Operational Technology systems are not amenable to the scanning approach: OT systems, such as those in water treatment facilities, operate continuously to maintain essential processes. Active scanning, which involves sending probes or interacting with system components, could disrupt operations, putting system services and functions at risk. Even a brief interruption could lead to cascading failures, such as delays in water purification or pressure irregularities in distribution systems, potentially jeopardizing public safety and service reliability.

Compounding this challenge is the prevalence of legacy systems within OT networks. Due to the critical nature of the services and functions provided, operators of these systems are understandably reluctant to introduce technological changes. Many water treatment plants rely on older technologies that predate modern cybersecurity standards. Such systems often lack even basic compatibility with contemporary scanning tools, rendering traditional vulnerability assessments impractical or even hazardous. Attempting to scan such components could destabilize them, further emphasizing the importance of caution when managing their security.

Of course, the inability to utilize traditional scanning approaches for vulnerability monitoring also has severe consequences. Without regular assessments, vulnerabilities may remain undetected, leaving these critical systems exposed to exploitation by cyber attackers. The 2021 human-error incident at a water treatment facility in Oldsmar, Florida, illustrates how unaddressed weaknesses can be exploited to manipulate processes, posing a threat to public health. This heightened risk underscores the urgency of finding viable security strategies for OT environments.

Alternative approaches to vulnerability management have been developed. Passive monitoring, for instance, provides a non-intrusive method for detecting anomalies by analyzing network traffic without directly interacting with OT components. Techniques that proactively model and assess a system for cybersecurity risks can identify potential vulnerabilities, prioritize them based on their impact, and recommend targeted mitigation efforts to reduce or eliminate those risks. Additionally, techniques such as network segmentation and virtual patching can isolate critical systems and shield them from known threats without necessitating disruptive changes.

The ASSURANT™ Suite is a tailored solution to these OT-specific challenges. By leveraging system modeling, attack-path analysis, and risk scoring technology, the ASSURANT™ Suite empowers water treatment facilities to strengthen their cybersecurity posture. It delivers actionable insights into the OT environment, facilitating proactive threat management while respecting the real-time constraints that define these systems.

The ASSURANT™ Suite ensures that municipal water treatment plants can safeguard their operations and protect public welfare in an increasingly complex and hostile cyber landscape.

2.2 MITIGATION OPTIMIZATION IN RISK MANAGEMENT

Comprehensive modeling of systems and identification of potential vulnerabilities are all well and good, but in the practical world, resources are limited, and compromises have to be made. In the realm of risk management, the ability to effectively mitigate threats while maximizing the use of limited resources is a constant challenge. Organizations face a diverse array of risks—ranging from cybersecurity breaches to naturally occurring operational disruptions—each

carrying its potential for harm. Yet, not all risks can or should be addressed with equal urgency or level of investment.

One of the key features of the ASSURANT™ Suite is its ability to guide the utilization of risk-management opportunities. Mitigation optimization offers a structured approach to prioritize and implement strategies that maximize risk reduction while minimizing costs. By carefully correlating risk scores with mitigation cost and effectiveness, decision-makers can ensure that their efforts are both impactful and efficient.

A risk score is a numerical representation of a threat's severity, calculated by combining the likelihood of an event occurring with the potential impact it could have. The higher the risk score, the more important it is to mitigate that risk. Situations assessed with a lower risk score may be safely set aside or assigned a lower priority.

For example, a cyberattack that is easily implemented and poses the possibility of significant damage (eg, shutting down a treatment facility) would garner a higher risk score. A cyberattack that is difficult to mount or otherwise unlikely to occur would garner a lower risk score, as would an attack that poses little or no damage. This score serves as a foundational metric, enabling organizations to rank risks and identify those that require immediate attention. However, simply knowing the risk score is not enough —mitigating every identified risk without discretion could lead to wasted resources or overburdened systems.

Mitigation optimization stands on twin pillars: cost and effectiveness. Mitigation cost refers to the financial or other resource investment required to implement a protective measure. Mitigation could be as straightforward as purchasing new software or as complex as funding the manpower needed to implement a comprehensive overhaul of processes. Effectiveness, on the other hand, measures how well a mitigation strategy reduces the risk score. A highly effective solution might drastically lower the likelihood or impact of a threat, while a less effective one might offer only marginal improvement. A mitigation that only senses an attack is less effective than one that actively repels it. The challenge for cybersecurity managers lies in balancing these two factors—investing in strategies that deliver the most significant risk reduction for the resources expended.

The key to optimization lies in correlating these elements: risk score, mitigation cost, and effectiveness. By analyzing this relationship, organizations can calculate a cost-effectiveness ratio, for instance, the reduction in risk score per dollar spent. Consider a scenario where two mitigation options are available to address a high-risk vulnerability. Option A costs $10,000 and reduces the risk score by 50 points, while Option B costs $5,000 but only reduces the risk score by 20 points. At first glance, Option A appears more effective, but a closer look reveals that Option A yields a reduction of 5 points per $1,000, whereas Option B achieves 4 points per $1,000. Depending on budget constraints and the desired level of risk reduction, Option B may prove to be the more intelligent choice. This type of analysis empowers organizations to make informed decisions, ensuring that mitigation efforts are neither overfunded nor underperforming.

In practice, this correlation can be applied across a portfolio of risks. Imagine an organization managing a network with multiple vulnerabilities: one with a risk score of 80 requiring a $20,000 mitigation that reduces the score by 60, and another with a score of 40 needing a $5,000 fix that cuts the score by 30. By comparing the cost-effectiveness of each—3 points per $1,000 for the first and 6 points per $1,000 for the second—the organization might prioritize the second mitigation, achieving a greater relative return on investment. Such an approach not only

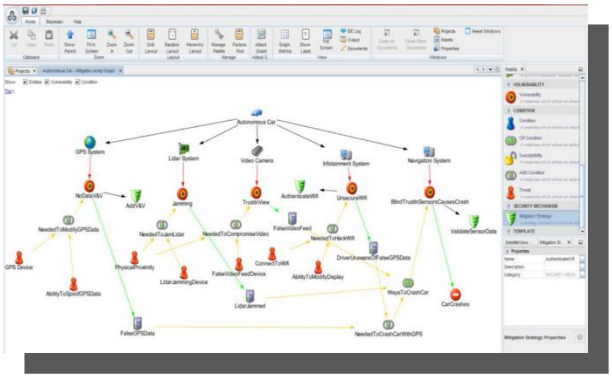
stretches limited resources further but also aligns mitigation efforts with the organization's overall risk tolerance and strategic goals.

Ultimately, mitigation optimization is about more than just mathematics—it's about making risk management practical and sustainable. By integrating risk scores with a precise evaluation of costs and effectiveness, organizations can move beyond reactive fixes and adopt a proactive, strategic stance. This method ensures that every dollar spent contributes meaningfully to safety and stability, turning the complex task of risk mitigation into a deliberate and optimized process.

3 THE ASSURANT™ SUITE: CAPABILITIES AND BENEFITS

The ASSURANT™ Suite is a cyber-physical system-focused toolset designed for modeling, visualizing, analyzing, and reporting on cyber-physical systems. Its key features address the gaps in the mentioned open source toolkit.

3.1 SYSTEM MODELING AND VISUALIZATION



In the increasingly complex landscape of cybersecurity, particularly within critical infrastructure such as municipal water treatment plants, accurately modeling and visualizing a system's architecture is paramount. The ASSURANT™ Suite excels in this domain by providing a comprehensive, passive representation of both IT and OT environments. This enables organizations to gain a deeper understanding of their systems without disrupting real-time operations.

Central to this capability is data flow modeling, which maps the intricate pathways through which data travels throughout the network. By charting these flows, ASSURANT™ reveals how information moves between components—such as SCADA systems, PLCs, and HMIs—highlighting potential points where data could be intercepted, manipulated, or exposed. This detailed mapping is crucial for identifying vulnerabilities that might otherwise remain hidden within the system's architecture.

Speaking of vulnerabilities, the ASSURANT™ Suite goes beyond mere identification of vulnerabilities; it offers robust vulnerability visualization tools that display weaknesses in a clear and actionable format. These visualizations pinpoint areas where the system is most susceptible to attacks—whether due to outdated software, misconfigurations, or unprotected interfaces—allowing cybersecurity teams to prioritize their efforts effectively.

Understanding vulnerabilities is only half the battle; addressing them efficiently is equally critical. To this end, the ASSURANT™ Suite offers mitigation visualization, enabling users to simulate and assess the impact of various mitigation strategies prior to implementation. By visually representing how different approaches—such as network segmentation, patch deployment, or

access control enhancements—can reduce risk, the ASSURANT™ Suite empowers decision-makers to choose the most effective solutions with confidence.

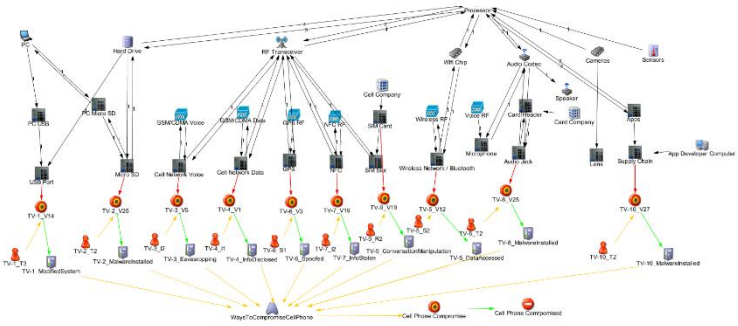
Together, these capabilities—data flow modeling, vulnerability visualization, and mitigation visualization—form a powerful triad that not only enhances situational awareness but also drives proactive, informed action in safeguarding critical infrastructure.

3.2 Advanced Cybersecurity Analyses

In today's rapidly evolving cybersecurity landscape, organizations must employ sophisticated analytical techniques to stay ahead of potential threats. In this section, we examine some of the critical analyses that form the foundation of a robust cybersecurity strategy.

Compromised data analysis involves the meticulous examination of data that has been accessed, altered, or exfiltrated by unauthorized entities. This analysis is crucial for understanding the extent of a breach, identifying the specific data affected, and determining the potential impact on the organization. By analyzing compromised data, security teams can develop targeted remediation strategies and prevent future incidents.

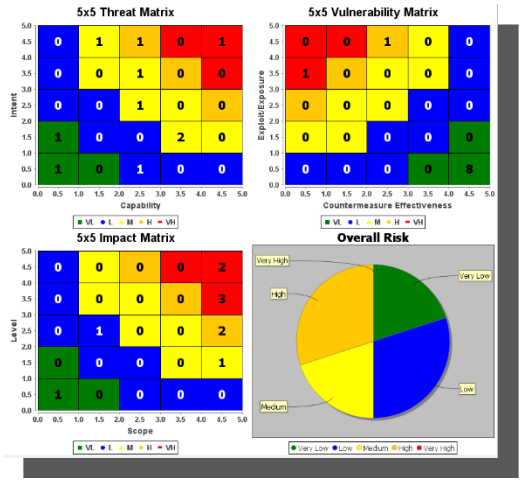
Modern software systems often rely on a complex web of third-party components and services. Compromised dependencies analysis focuses on identifying vulnerabilities within these external elements that could be exploited to gain unauthorized access to the system. This analysis is essential for maintaining the integrity of the entire software ecosystem and ensuring that security measures extend beyond the organization's immediate control.



Beyond examining external dependencies, it is equally important to assess the risks to internal assets. Target risk analysis evaluates the potential threats to specific assets or systems within an organization. By considering factors such as the asset's value, its exposure to potential attackers, and existing security controls, this analysis helps prioritize security efforts and allocate resources effectively. Understanding the risk profile of key targets enables organizations to focus their defenses where they are most needed.

Understanding the risks to individual targets is crucial, but it is also essential to consider how attackers might navigate through the system. Attack path clustering involves grouping similar sequences of actions that attackers might take to compromise a system. By identifying common patterns or vulnerabilities across multiple potential attack paths, security teams can develop more efficient and comprehensive defense strategies. This approach not only helps mitigate current threats but also anticipates and prevents future attacks.

To enhance the timeliness and relevance of threat detection, the ASSURANT™ Suite can generate near-real-time alerts through automated ingestion and correlation of published vulnerability disclosures and related threat intelligence, subject to source availability, relevance, and feed latency. This approach helps security teams identify newly published threats relevant to the modeled environment soon after those disclosures are ingested and correlated, allowing for swift action to protect the organization's assets. While not instantaneous, this near-real-time capability strikes a balance between immediacy and the practical constraints of monitoring and analyzing a vast array of vulnerability data sources.



3.3 Vulnerability Management

In the dynamic realm of cybersecurity, staying ahead of emerging threats requires constant vigilance and adaptability. The ASSURANT™ Suite addresses this need by incorporating an automated process for updating vulnerabilities within its system models as new ones are identified and published. This capability ensures that the cybersecurity framework remains current, reflecting the latest threats identified by industry sources such as the National Vulnerability Database (NVD) or MITRE's CVE listings. Each time a new vulnerability is disclosed, the system seamlessly integrates this information into its existing models, providing an up-to-date representation of potential risks without manual intervention.

This automation begins with the continuous ingestion of vulnerability data feeds, which are monitored in real-time to capture the latest updates. As new CVEs are published, ASSURANT™ evaluates their relevance to the modeled environment—considering factors such as affected software versions, system components, and operational contexts specific to municipal water treatment plants. This evaluation triggers an immediate update to the model, appending details such as the vulnerability's severity, potential exploitability, and recommended mitigation steps. By doing so, the system ensures that security teams are constantly working with the most recent threat intelligence, reducing the window of exposure to newly discovered weaknesses.

The benefit of this automated update process is significant: delays associated with manual updates are eliminated. Human oversight often lags behind the rapid pace of vulnerability disclosures, which sometimes number in the dozens daily. For instance, a newly published vulnerability affecting a widely used SCADA software package could be integrated into the model within hours, enabling proactive adjustments to defense strategies. This real-time adaptability is particularly critical for OT environments, where even a brief delay could leave critical infrastructure exposed to exploitation. Moreover, the automated updates enhance the accuracy of risk assessments and attack path analyses, ensuring that mitigation efforts target the most current threats.

This feature also supports a proactive cybersecurity posture by fostering continuous improvement. As the model evolves with each vulnerability update, it provides a living blueprint of the system's security landscape. Security teams can leverage the updated model to simulate the impact of new threats, refine their risk scoring, and adjust mitigation priorities—all without the need to rebuild the analyses from scratch.

As the cybersecurity community grapples with an ever-growing list of published vulnerabilities, this automated process positions the ASSURANT™ Suite as a vital tool for maintaining the resilience of municipal water treatment plants against an unrelenting tide of cyber risks.

3.4 RISK SCORING

In the ever-evolving field of cybersecurity, accurately assessing and mitigating risks is crucial for protecting critical infrastructure such as municipal water treatment plants. The ASSURANT™ Suite elevates this process through sophisticated risk-scoring mechanisms and advanced mitigation strategies tailored to the unique demands of OT environments. At the heart of this approach lies integration with MITRE D3FEND, a knowledge base and knowledge graph of defensive cybersecurity techniques and their relationships to adversary techniques. D3FEND can support defensive analysis and control mapping, but it should not be described as a risk-description standard or as a measure of control effectiveness. By aligning with MITRE D3FEND, the ASSURANT™ Suite leverages a structured methodology to evaluate risks based on established defensive countermeasures, including network segmentation, access control, and threat detection. This integration ensures that risk scores reflect not only the likelihood and impact of potential attacks but also the effectiveness of existing defenses, offering a holistic view that guides strategic decision-making.

Beyond risk assessment, the ASSURANT™ suite employs optimization mitigation algorithms to enhance the efficiency of resource allocation. These algorithms analyze a range of factors to recommend the most effective mitigation strategies, striking a balance between risk reduction and practical constraints. A key component of this process is considering cost drivers—elements that influence the financial and operational investment required for mitigation. These drivers include the expense of hardware upgrades, software licenses, personnel training, and downtime during implementation. By factoring in these costs, the algorithms prioritize solutions that deliver the most significant risk reduction per unit of expenditure, ensuring that limited budgets are utilized to their fullest potential. For instance, a mitigation option involving a low-cost configuration change might be favored over an expensive system overhaul if both achieve comparable risk reduction, as determined by the algorithm's analysis.

This cost-driven optimization becomes particularly valuable in scenarios where multiple vulnerabilities compete for attention. With cybersecurity budgets under scrutiny and threats proliferating, the ASSURANT™ Suite's algorithms can evaluate a portfolio of risks—such as an exposed SCADA interface or a misconfigured PLC—and recommend a sequence of mitigations that maximizes overall security while minimizing financial impact. The result is a dynamic, data-informed approach that adapts to the specific cost structures and operational realities of water treatment facilities.

By combining MITRE D3FEND's defensive insights with optimization algorithms that account for cost drivers, the ASSURANT™ Suite empowers organizations to strengthen their cybersecurity

posture efficiently and effectively, safeguarding critical operations against an ever-growing array of cyber threats.

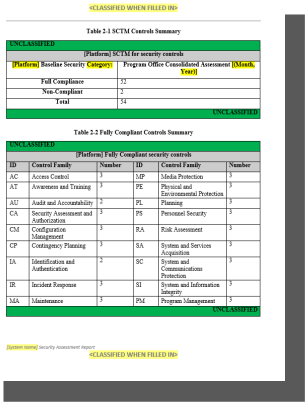
3.5 COMPLIANCE REPORTING

The reality of cybersecurity management is that it is both a technical and a bureaucratic process. In addition to identifying vulnerabilities and implementing appropriate mitigations to protect against them, standards must be adhered to, regulations must be followed, and reports demonstrating compliance must be published. In the realm of cybersecurity for critical infrastructure, adherence to established compliance standards is not just a regulatory requirement but is the cornerstone of operational trust and resilience. The urgency of maintaining compliance has intensified amid rising cyber threats, making automated and accurate reporting indispensable. The ASSURANT™ Suite can support evidence generation, control mapping, and audit preparation for applicable frameworks and requirements.

Developed by the AICPA, a SOC 2 examination is an attestation report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy. The ASSURANT™ Suite facilitates compliance by generating detailed reports that document the controls and processes that are in place to protect OT and IT environments, ensuring that water treatment facilities meet the stringent criteria for trusted service. These reports provide evidence of continuous monitoring and risk management, which are critical for audits and for maintaining customer confidence in the face of potential breaches.

ISO 27001, an internationally recognized standard for Information Security Management Systems, provides a systematic approach to managing sensitive company information. The ASSURANT™ Suite supports compliance with this standard by producing automated documentation that outlines risk assessments, security policies, and mitigation strategies. This capability streamlines the process of achieving and sustaining ISO 27001 certification, enabling facilities to demonstrate a commitment to best practices in information security. The suite's ability to update models with new vulnerabilities ensures that compliance documentation evolves in real time, keeping pace with the standard's emphasis on continuous improvement.

Additionally, the ASSURANT™ suite extends its compliance reporting capabilities to include support for NIST 800-53 Revision 4 and Revision 5, the widely adopted frameworks for federal information security. These revisions provide comprehensive security controls and guidelines for protecting information systems, with Revision 5 introducing enhanced risk management and supply chain security measures. The ASSURANT™ Suite automates the generation of reports that map the plant's security controls to NIST 800-53 controls, including access control (AC), incident response (IR), and system and communications protection (SC). By integrating real-time vulnerability updates and risk scores into these reports, the ASSURANT™ Suite ensures alignment with both Revision 4's foundational controls and Revision 5's expanded focus on privacy and resilience, facilitating compliance audits and supporting Authority to Operate (ATO) processes.



The ASSURANT™ Suite's reporting engine provides a unified solution that reduces the burden of manual reporting while ensuring accuracy and consistency. Automated exports in formats such as Microsoft

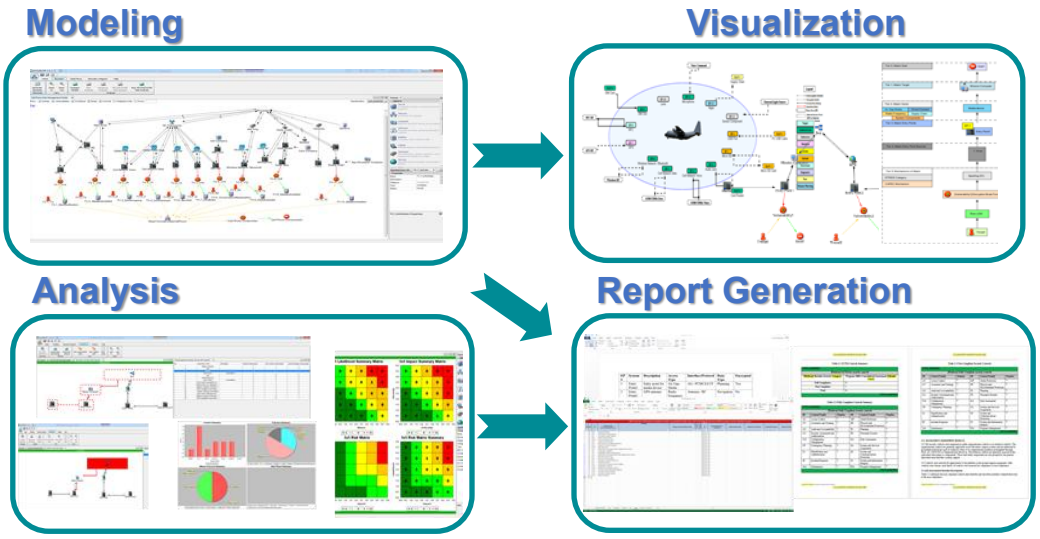
Word and CycloneDX JSON enable seamless submission to regulatory bodies and auditors. Customizable templates allow users to tailor reports to their specific compliance needs. This comprehensive approach not only meets current regulatory demands but also positions water treatment plants to adapt to future standards, fostering a proactive stance against the evolving cyber threat landscape.

4 USE CASE: ASSURANT™ IN MUNICIPAL WATER TREATMENT PLANTS

The Cranberry Water Treatment Plant, located in Westminster, Maryland, is part of the city's drinking water system and supports water treatment and distribution functions through a complex network of operational technology (OT) and information technology (IT) systems. The facility faces an escalating threat landscape, exemplified by incidents such as the 2021 Oldsmar, Florida, attack and the 2024 Arkansas City breach, which exposed vulnerabilities in SCADA systems and HMIs.

4.1 USE CASE OVERVIEW

This use case demonstrates the deployment of the ASSURANT™ Suite to enhance the cybersecurity resilience of the Cranberry Water Treatment Plant. The facility's architecture features networked SCADA systems, PLCs, HMIs, and workstations, which are monitored using existing open-source tools. The ASSURANT™ Suite integrates with this framework to provide a passive, visualized system model, advanced analyses, risk-based evaluations, and automated compliance reports. The process unfolds in five key phases: modeling, documentation, analysis, evaluation, and reporting, each tailored to the plant's real-time OT constraints and regulatory requirements.



4.1.1 Modeling the System

The ASSURANT™ Suite begins by constructing a detailed data flow model of the Cranberry Water Treatment Plant's OT/IT environment. This model maps the movement of data between

SCADA systems, PLCs, HMIs, and networked sensors, identifying undocumented legacy components that evade traditional scans due to their real-time nature. Vulnerability visualization within the model highlights exposed interfaces and misconfigured systems, while mitigation visualization simulates network segmentation and patch deployment, ensuring minimal disruption. This initial modeling phase, completed within the first week of deployment, provides a foundational blueprint for subsequent analyses.

4.1.2 Documenting the Environment

Documentation is automated as the ASSURANT™ Suite updates its model with newly published vulnerabilities from sources such as the National Vulnerability Database (NVD) and MITRE CVE listings. The system integrates a recent vulnerability affecting a widely used SCADA software, appending severity scores and mitigation recommendations. Compromised data analysis documents the potential impact of a breach, while compromised dependencies analysis identifies risks in third-party PLC firmware. This living documentation, exportable in Microsoft Word and CycloneDX JSON formats, ensures a continuously updated record of the plant's security state.

4.1.3 Analyzing Threats

The ASSURANT™ Suite conducts advanced analyses to uncover potential threats. Compromised data analysis reveals the extent of data exfiltration risks from exposed HMIs, while compromised dependencies analysis flags vulnerable third-party components. Target risk analysis evaluates the criticality of SCADA systems, assigning high risk scores based on their impact on water purification processes. Attack path clustering groups similar exploitation routes—such as lateral movement from workstations to PLCs—enabling the identification of common vulnerabilities. Near real-time alerts, driven by continuous monitoring of published vulnerabilities, notify the team of a new CVE affecting PLC firmware within hours of its release, facilitating swift response.

4.1.4 Evaluating Risks and Mitigations

Risk scoring integrates MITRE D3FEND countermeasures to evaluate the effectiveness of existing defenses; for example, assigning a risk score of 75 out of 100 to an exposed SCADA interface due to its high impact and moderate exploitability. Optimization mitigation algorithms then correlate this score with cost drivers, such as $15,000 for a hardware upgrade versus $2,000 for a configuration change, recommending the latter due to its 60-point risk reduction, which is available at a lower cost. Mitigation visualization simulates these options, showing that network segmentation would reduce the risk score by 50 points with minimal downtime. This evaluation, completed over two weeks, guides the plant's cybersecurity team in prioritizing cost-effective strategies.

4.1.5 Reporting Compliance

The ASSURANT™ Suite generates automated compliance reports aligned with SOC 2 and ISO 27001 standards. SOC 2 reports document controls for data confidentiality, ISO 27001 reports detail risk management policies, and reports verify asset protection measures, all tailored to the plant's OT network. A report export highlights compliance with EPA cybersecurity standards, putting the Cranberry facility ahead of the 70% noncompliance rate among water treatment systems. These reports, submitted to regulatory bodies, streamline audits and demonstrate adherence to federal mandates, enhancing the plant's operational trust.

4.1.6 Integration with Open Source Tools

The ASSURANT™ Suite complements an open-source architecture by enhancing Suricata with attack path visualization, Sysmon/Winlogbeat with vulnerability tracking, and Elasticsearch/Kibana with unified data analysis. Apache NiFi integrates data flows into the ASSURANT™ Suite's model, ensuring compatibility with existing workflows. This synergy, tested over a one-month pilot, amplifies the plant's monitoring capabilities without requiring a complete system overhaul.

4.2 Expected Outcomes

- Enhanced Visibility: Data flow modeling uncovers hidden legacy components, improving situational awareness.
- Proactive Defense: Attack path clustering and near real-time alerts reduce exposure to threats like the 2024 Kansas breach.
- Cost Efficiency: Optimization algorithms save $10,000 by prioritizing low-cost mitigations.
- Regulatory Compliance: Automated reports meet SOC 2 and ISO27001 requirements, avoiding penalties.

4.3 Conclusion

The ASSURANT™ Suite would transform the cyber-security posture of the Cranberry Water Treatment Plant by modeling its environment, documenting threats, analyzing risks, evaluating mitigations, and reporting compliance. This holistic approach, when integrated with open-source cyber analysis and monitoring tools, will ensure resilience against evolving cyber threats while meeting regulatory requirements.

5 References

- Knowledge Based Systems, Inc. (2024). ASSURANT™ Suite. Retrieved from www.assurantcyber.com.
- U.S. Cybersecurity and Infrastructure Security Agency (CISA). (2024). Water and Wastewater Cybersecurity. Retrieved from www.cisa.gov.
- U.S. Environmental Protection Agency (EPA). (2024). Cybersecurity for the Water Sector. Retrieved from www.epa.gov.
- Johns Hopkins University Applied Physics Laboratory. (2023). Developing Cybersecurity Solutions for Industrial Infrastructures. Retrieved from www.jhuapl.edu.
- Industrial Cyber. (2024). US EPA Report Cites Cybersecurity Flaws in Drinking Water Systems. Retrieved from industrialcyber.co.