2026

Operational Technology (OT) Cybersecurity in Natural Gas and Oil Refineries

Shawn Reynolds

4/21/2026

Executive Summary

Operational technology (OT) controls the core industrial processes in natural gas and oil refineries, including the automation, monitoring, and control of complex, hazardous, and high-value industrial systems.[1]

As refinery operators connect OT environments more closely with business systems, remote access services, analytics platforms, and third-party support channels, the traditional assumption of OT isolation becomes less reliable, and the attack surface expands. Incidents such as the Colonial Pipeline ransomware event and the TRITON/TRISIS attack on a safety instrumented system illustrate that OT cybersecurity failures can disrupt operations, drive regulatory action, and, in some cases, create safety and environmental risks in addition to financial and reputational harm.[2][3]

This whitepaper examines the cybersecurity challenges, operational risks, and threat vectors most relevant to oil and gas refinery OT environments. It reviews representative incidents, widely used security frameworks, and practical controls for segmentation, asset visibility, vulnerability management, and incident response. The ASSURANT™ Cyber-Physical Security suite, from Knowledge Based Systems, Inc. (KBSI), is a model-based platform that helps operators document OT environments, evaluate security dependencies, and support risk-informed decision-making.

By combining system modeling, visualization, scenario analysis, and reporting, the platform helps teams improve visibility, validate design assumptions, and prioritize mitigation efforts across connected IT and OT environments.

Architecture of Operational Technology in Oil & Gas Refineries

Natural gas and oil refineries rely on a layered OT architecture that integrates industrial control systems (ICS), supervisory control and data acquisition (SCADA), distributed control systems (DCS), safety instrumented systems (SIS), programmable logic controllers (PLCs), and a complex network of sensors and actuators. Each of these elements plays a vital role in ensuring safe, reliable, and efficient production, from feedstock intake and process operations to storage, distribution, and environmental controls.

The Purdue Enterprise Reference Architecture (PERA) is commonly used to conceptualize refinery OT environments. PERA segments control functions into multi-level zones, which support defense-in-depth and make lateral movement more difficult for adversaries.**Error! Reference source not found.**

Purdue Level	Systems/Functions	Security Measures
0-1	Physical processes, sensors, actuators, PLCs	Physical locks, device hardening
2	Local control, HMI, SCADA	Role-based access controls, segmentation
3	Site operations, historians, alarm servers	DMZ, IDS/IPS
3.5	OT/IT demilitarized zone	Firewalls, data diodes, protocol breaks
4-5	Business networks, ERP, analytics	NGFWs, application-level filtering

1 National Petroleum Council, “Purdue Model Framework for Industrial Control Systems & Cybersecurity Segmentation,” Topic Paper no. 4-14, in Dynamic Delivery—America’s Evolving Oil and Natural Gas Transportation Infrastructure (Washington, DC: National Petroleum Council, December 12, 2019)

[2] CISA, "AA21-131A: DarkSide Ransomware Impacting Colonial Pipeline", 2021.

[3] Mandiant, "Attackers Deploy TRITON Malware Targeting Safety Systems", 2018.

Emerging Risks and Threat Landscape

OT systems differ from traditional enterprise IT in ways that materially affect cybersecurity priorities and defensive options:

- **Long asset lifecycles:** Refineries often operate control systems for 15-30 years, which can leave legacy equipment in service long after established security controls have been updated, revised, or replaced.
- **Safety and availability priorities:** In OT, safe and continuous operation usually takes precedence over rapid patching or frequent architectural change.
- **Constrained maintenance windows:** Updates are often delayed until planned outages or validation cycles, extending the exposure window for known weaknesses.
- **Legacy industrial protocols:** Protocols such as Modbus and DNP3 were not designed with modern authentication and encryption expectations in mind.
- **Limited visibility:** Many OT environments still lack complete asset inventories, normalized logging, and monitoring coverage across older devices.
- **Increasing IT-OT interdependence:** Connections to historians, analytics systems, vendor support paths, and enterprise applications increase operational value but also create additional trust relationships that must be secured.

Because disruption in the oil and gas sector can have operational, economic, and public-impact consequences, the sector remains a persistent target for both criminal and state-aligned cyber actors. Recent OT threat reporting describes continued ransomware pressure on industrial organizations, ongoing state-linked targeting of critical infrastructure, increased concern over remote and third-party access, and weak segmentation.[4][5]

In practice, many impactful incidents still begin with familiar weaknesses such as exposed remote services, stolen credentials, poor identity controls, or insufficient separation between enterprise and operational networks.

Public reporting from OT security vendors and government agencies consistently points to the following common attack paths and exposure areas:

- **Remote access exploitation:** Weakly secured VPNs, remote desktop services, and vendor support connections continue to provide common initial access paths.
- **Ransomware and operational disruption:** Even when malware first affects enterprise systems, the operational impact can extend into OT through shutdown decisions, shared services, or loss of visibility.
- **OT-cloud and third-party integration risk:** Cloud-connected applications, external analytics, and contractor-managed services increase dependency on identity, configuration, and supplier security.
- **Supply-chain compromise:** Trusted vendors, software providers, and integrators can become pathways into refinery environments when upstream controls fail.
- **State-linked intrusion activity:** Threat actors focused on critical infrastructure often seek persistence, reconnaissance, and pre-positioning rather than immediate disruption.**Error! Reference source not found.Error! Reference source not found.**

[4] Dragos, "ICS/OT Cybersecurity Year in Review 2023--2024", Dragos Inc., 2024.

[5] Microsoft, "Volt Typhoon Targets U.S. Critical Infrastructure", 2017.

Selected Key OT Cybersecurity Risks	Example Impact/Concern	Real-World Illustrations
Ransomware	Production shutdown, extortion	Colonial Pipeline, 2021 **Error! Reference source not found.**
Remote access compromise	Lateral movement to OT/ICS	Volt Typhoon activity and related critical-infrastructure targeting reports, 2023-2025[5]
Safety system attacks	SIS/ESD disablement, unsafe state	Triton/Trisis, Saudi refinery, 2017 [3]
Insider/contractor misuse	Unauthorized changes, sabotage	Examples from water-sector insider or operator misuse cases
Poor asset visibility	Blind spots for threat detection	Common across refineries
Supply chain attack	Introduction of malware/backdoor	SolarWinds and other third-party compromise cases affecting trust relationships

Recent Cyber Incidents in the Oil & Gas Sector

Colonial Pipeline Ransomware Attack

In May 2021, the Colonial Pipeline ransomware attack catalyzed sweeping reforms across the industry. The DarkSide group gained access via a compromised VPN account that lacked multi-factor authentication and targeted IT systems. The preemptive shutdown of pipeline operations to contain the incident led to severe fuel shortages, public concern, and economic disruption on the U.S. East Coast.[2]

Key lessons included the following:

- **IT-OT interdependence introduces new risks:** The attack path began in the IT domain, but the shutdown decision highlighted how tightly business and operational functions can be linked.
- **Segmentation matters:** The event heightened industry concern around lateral movement and the need for clearer separation between enterprise and operational environments.
- **Regulatory consequences can be immediate:** Post-incident directives increased expectations for assessments, segmentation, incident reporting, and response planning for regulated pipeline operators. [2]

Triton/Trisis SIS Malware

In 2017, the Triton malware incident at a Saudi Arabian refinery marked the first publicly documented attempt to manipulate a safety instrumented system with potentially catastrophic consequences. Attackers gained access to Schneider Electric Triconex SIS engineering systems and attempted to interfere with fail-safe logic associated with refinery shutdown functions. Although the attack was interrupted by a protective fail-safe condition, the case demonstrated that OT cyber compromise can create direct process-safety risk.[3]

Implications included the following:

- **Physical consequence was a primary concern:** Targeting SIS raised the possibility of injury, explosion, or environmental harm.
- **Access paths may involve multiple weaknesses:** Investigators and analysts have associated incidents of this type with a mix of remote access weakness, poor segmentation, and detailed operational knowledge.
- **Long dwell time remains a challenge:** OT intrusions may involve extended reconnaissance before disruptive action occurs. 3

Additional Incidents and Trends

Recent incidents further illustrate the range of actors and motives affecting critical infrastructure:

- **BAZAN Group, Israel (2023):** Publicly claimed hacktivist activity highlighted the role of geopolitics and publicity-seeking intrusion campaigns in industrial sectors.
- **Oldsmar Water (2021) and similar remote-access cases:** These incidents underscored the risk created by weak access controls and poor exposure management across critical infrastructure environments.

Securing OT Infrastructure: Best Practices and Industry Guidance

Network Segmentation

Segmentation is a foundational OT security control because it limits an attacker's ability to move laterally across connected environments. Instead of flat architectures, refineries should implement layered zones and conduits as defined in the ISA/IEC 62443 standards and the Purdue model.[6]

Segmentation Approach	Scope	Security Benefits	Limitations
VLAN-based (L2)	Broadcast domains	Some restrictions, limited payload control	Lateral movement is still possible
Subnet-based (L3)	IP-based zones	Isolates groups, manageable boundaries	Can become brittle and operationally rigid
NGFW and micro-segmentation (L7/L3)	Application-level	Deeper visibility, stronger control over pathways	More complex, requires expertise

Best practices include the following:

- Map and categorize assets by process criticality and function, such as SIS, DCS, SCADA, and field I/O.
- Establish DMZs between IT and OT and strictly control all crossing conduits through proxies, firewalls, and protocol validation.
- Use security controls that understand industrial protocols where operationally feasible.
- Apply tighter segmentation to high-risk process areas.
- Maintain strict remote access controls, including least privilege, MFA, approval workflows, and logging.[6]

[6] ISA, "ISA/IEC 62443 Series: Security for Industrial Automation and Control Systems", ISA, 2018.

Asset Visibility and Inventory

Without a current asset inventory, organizations lack the visibility needed to prioritize monitoring, response, and remediation. Key recommendations include the following.[7]

- Continuously identify devices, software, and connections within the OT environment, including legacy and shadow assets.
- Classify assets by criticality and function.
- Capture attributes such as firmware, software versions, communication protocols, location, and operational status.
- Prioritize the most critical assets for enhanced monitoring and compensating controls.[7]

Asset Management Best Practices	Measures/Indicators
Comprehensive inventory	Near-complete asset coverage with relevant attributes
Automated discovery and scanning	Tools for passive discovery and behavioral mapping
Categorization by role/criticality	Zones and critical process areas identified.
Continuous monitoring	Real-time updates and anomaly alerts
Documentation and reporting	Inventory linked to governance and compliance documentation

Vulnerability Management

With a substantial rise in OT vulnerability reporting in recent years, refineries should adopt a risk-based approach to vulnerability management rather than relying solely on patching.[8]

- **Continuous monitoring:** Correlate asset inventories with CVE databases and the CISA Known Exploited Vulnerabilities catalog.
- **Prioritization:** Focus on high-criticality and externally exposed assets first.
- **Mitigation planning:** Where patching is impractical, use compensating controls such as isolation, restricted access, protocol filtering, or additional monitoring.[8]

Incident Response Planning

Incident response in OT environments differs sharply from enterprise IT response, as operators must consider process safety, environmental impact, and operational continuity alongside digital containment.[9]

- **Preparation:** Develop playbooks for enterprise compromise, ransomware affecting OT-dependent operations, and unexplained operational downtime.
- **Team structure:** Establish a clear command structure with defined technical, operational, and executive roles.
- **Integration with process safety:** Plans should account for physical consequences, not just technical recovery.
- **OT forensics readiness:** Prepare to gather process data, sequence-of-events records, diagnostics, and device logs.
- **Regular tabletop exercises:** Test separation of enterprise and OT environments, recovery decision points, and authority chains.[9]

[7] CISA, "Cross-Sector Cybersecurity Performance Goals (CPGs)", 2022.

[8] SynSaber, "ICS Vulnerability Report: Findings from CISA ICS Advisories", 2023.

Standards and Regulatory Frameworks

A mix of standards, guidance, and sector-specific expectations, including the following, shapes refinery cybersecurity programs:

- **ISA/IEC 62443:** A widely used framework for industrial automation and control system security, emphasizing zones, conduits, and lifecycle security practices.[6]
- **NIST SP 800-82:** U.S. guidance for securing industrial control systems.[9]
- **TSA pipeline directives (post-Colonial):** Requirements and expectations for regulated U.S. pipeline operators related to assessments, segmentation, incident reporting, and response.[2]
- **CISA Cybersecurity Performance Goals:** Baseline objectives for critical infrastructure organizations. [7]
- **ISO 22320/22361 concepts:** Incident-management practices increasingly referenced in emergency and resilience planning.

These frameworks are most useful when organizations turn them into operational procedures, architecture standards, repeatable reviews, and current documentation.

IT-OT Convergence and Its Security Implications

The Drivers and Benefits

IT-OT convergence enables the following:

- Real-time process analytics and predictive maintenance, which can reduce unplanned downtime and improve asset utilization.
- Better correlation of process and business data to support efficiency, planning, and automation initiatives.[10]

The Security Risks

- **Expanded attack surface:** Internet-connected or enterprise-connected assets create additional entry points.
- **Loss of assumed isolation:** Legacy expectations of air-gapped OT environments often no longer apply.
- **Data flow complexity:** More integrations make monitoring, trust management, and troubleshooting harder.
- **Talent and change-management challenges:** Blending IT and OT practices remains difficult for many organizations.

Countermeasures

- **Zero trust principles:** Apply strong authentication, MFA, and least privilege for each user, device, and connection.
- **Unified monitoring and anomaly detection:** Correlate OT and IT telemetry where operationally feasible.
- **Policy-driven integration:** Subject new connections and integrations to documented security review.

[9] National Institute of Standards and Technology, Guide to Operational Technology (OT) Security, Special Publication 800-82, Rev. 3 (Gaithersburg, MD: National Institute of Standards and Technology, September 2023),
[10] IBM, "X-Force Threat Intelligence Index 2024", IBM Security, 2024.

Trends and Future Directions

AI-Driven Threats and Defense

Analysts increasingly expect threat actors to use automation and AI-assisted workflows to accelerate reconnaissance, improve phishing, and scale intrusion operations. At the same time, defenders are using analytics, anomaly detection, and workflow automation to improve early warning and investigation speed.[11]

Supply Chain and Third-Party Risk

Attention is shifting beyond direct network defense to vendor validation, software provenance, and third-party access governance across the refinery ecosystem.

IT-OT Unified Security Operations Centers

More organizations are building OT-aware security operations models that combine IT and OT telemetry while retaining OT-specific procedures and expertise.

Continuous Compliance and Regulation

Compliance expectations continue to evolve, requiring refinery operators to keep architecture documentation, incident procedures, and governance evidence current.[7]

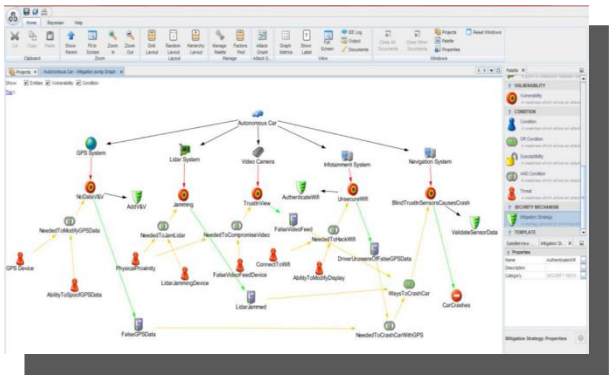
Changing Workforce Needs

Persistent shortages of cyber-aware OT personnel are increasing demand for tools that help teams document systems, understand dependencies, and communicate risk more efficiently.

KBSI's ASSURANT™ Cyber-Physical Security Suite

Understand the Risk Before It Finds You

The ASSURANT™ suite from KBSI is a model-based cyber-physical security and risk management platform for complex environments such as refineries. In the context of this paper, its value is best described in terms of documentation, modeling, dependency analysis, and planning support rather than as a standalone control that directly prevents every category of attack.



Key capabilities of the suite include the following:

- **Model-based architecture mapping:** Supports creation of structured representations of IT and OT architectures at the system and component level.
- **Asset inventory support:** Helps teams consolidate asset information and identify documentation gaps, including for low-change or legacy assets.
- **Visualization:** Provides visual representations of networks, assets, trust boundaries, and dependencies to support collaboration across OT, IT, and management stakeholders.
- **Risk analysis:** Supports attack-path and scenario analysis to help prioritize high-consequence exposures and evaluate mitigation options.
- **Vulnerability context:** Can be aligned with CVE, KEV, and vendor advisory information to connect published vulnerabilities to modeled assets and dependencies.
- **Scenario testing:** Enables what-if analysis for segmentation, access pathways, and potential attack progression before operational changes are made.
- **Reporting support:** Supports production of reports and compliance-oriented documentation to reduce manual documentation effort.

[11] Mandiant, "M-Trends 2024: Insights from Frontline Incident Response", 2024.

- **Integrations:** Are intended to exchange data with asset discovery, monitoring, SIEM, and vulnerability-management tooling where those integrations are available.

Asset Visibility and Documentation

The ASSURANT™ suite helps operators maintain a more complete and current view of assets across environments, including legacy DCS and SCADA systems as well as newer connected sensors and support systems. By organizing asset, relationship, and dependency data in a common model, the suite supports inventory reviews, architecture documentation, and evidence preparation for internal governance or external compliance activities.

Network Segmentation and Attack Path Analysis

The suite can be used to model existing and proposed segmentation approaches, evaluate trust boundaries, and analyze possible lateral movement paths across interconnected refinery systems. This supports design review by helping teams test whether critical control zones appear adequately separated, whether DMZ assumptions hold, and where policy or routing decisions may create unintended paths between business and operational environments.

Vulnerability and Policy Management

The ASSURANT™ suite can correlate vulnerability information with asset records and modeled dependencies, enabling teams to assess where published weaknesses may matter operationally. For assets that cannot be patched quickly, the model can also support evaluation of compensating controls such as tighter access restrictions, additional monitoring, or stronger segmentation.

Incident Response Support

By documenting asset relationships, process dependencies, and likely attack paths in advance, the ASSURANT™ suite supports more structured incident planning and exercise design. During tabletop exercises or incident review, that documentation can help teams identify affected systems, evaluate containment options, and communicate operational implications to technical and non-technical stakeholders.

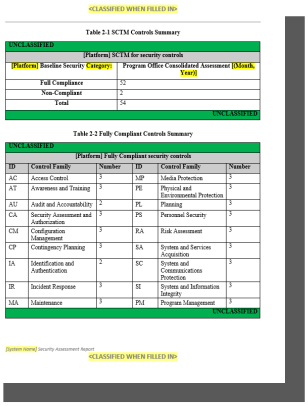

«CLASSIFIED WHEN FILLED IN»

Table 2-1 SCTM Controls Summary

UNCLASSIFIED	
[Platform] SCTM for security controls	
[Platform] Baseline Security Category	Program Office Consolidated Assessment [Month, Year]
Full Compliance	52
Non-Compliant	2
Total	54
UNCLASSIFIED	

Table 2-2 Fully Compliant Controls Summary

UNCLASSIFIED					
[Platform] Fully Compliant security controls					
ID	Control Family	Number	ID	Control Family	Number
AC	Access Control	3	MP	Media Protection	3
AT	Awareness and Training	3	PE	Physical and Environmental Protection	3
AU	Audit and Accountability	2	PL	Planning	3
CA	Security Assessment and Authorization	3	PS	Personnel Security	3
CM	Configuration Management	3	RA	Risk Assessment	3
CP	Contingency Planning	3	SA	System and Services Acquisition	3
IA	Identification and Authentication	2	SC	System and Communications Protection	3
IR	Incident Response	3	SI	System and Information Integrity	3
MA	Maintenance	3	PM	Program Management	3
UNCLASSIFIED					

[System Name] Security Assessment Report
«CLASSIFIED WHEN FILLED IN»

Regulatory and Executive Communication

The ASSURANT™ suite supports the preparation of graphics, architectural views, and narrative reports for governance, compliance, and executive communication workflows. This can help operational, cybersecurity, and leadership stakeholders work from a more consistent representation of risk, architecture, and remediation status.

IT-OT Convergence

The ASSURANT™ suite supports modeling of relationships and dependencies between IT and OT systems. Analysis of integration points can help operators identify hidden trust relationships, evaluate zero-trust design assumptions, and improve documentation of IT-OT interfaces for security review and compliance support.

Summary

In refinery environments, ASSURANT™ should be positioned as a model-based planning and analysis layer that helps teams document OT architecture, evaluate dependencies, understand how vulnerabilities and trust relationships intersect, and communicate mitigation priorities across technical and management audiences.

The platform supports and enables several practices discussed in this paper:

- **Modeling:** Digitally map the network, visualize connections, and test segmentation scenarios.

- **Policy validation:** Identify potentially insecure paths and evaluate segmentation intent against modeled relationships.
- **Regulatory documentation:** Generate reports and supporting artifacts that help demonstrate due diligence in architecture review, incident planning, and governance activities.

Key OT Security Vendors and Industry Solutions

KBSI's ASSURANT™ suite can complement the offerings of leading companies delivering OT security solutions for refineries:

Vendor	Focus/Key Capabilities	Suitability/Strength
Nozomi Networks	Asset discovery, visualization, and real-time monitoring	OT/IoT focus, non-intrusive
Claroty	Deep packet inspection, secure remote access, vulnerability management	Strong compliance, analytics
Fortinet	Scalable NGFWs, segmentation, OT protocol protection	Integration, industry partnerships
Honeywell Forge	Continuous monitoring, threat prioritization	Deep industrial knowledge
Dragos	Threat intelligence, incident response, asset mapping	OT/ICS specialization
Siemens / ABB / Schneider Electric	Physical and cyber defense, integration with process hardware	Holistic, system-level solutions
Cisco	IT-OT integration, NGFW, endpoint, and network defense	Enterprise-scale, hybrid networks
Waterfall, Tenable, SCADAfence, others	Unidirectional gateways, vulnerability management, and non-intrusive monitoring	Specialized use cases

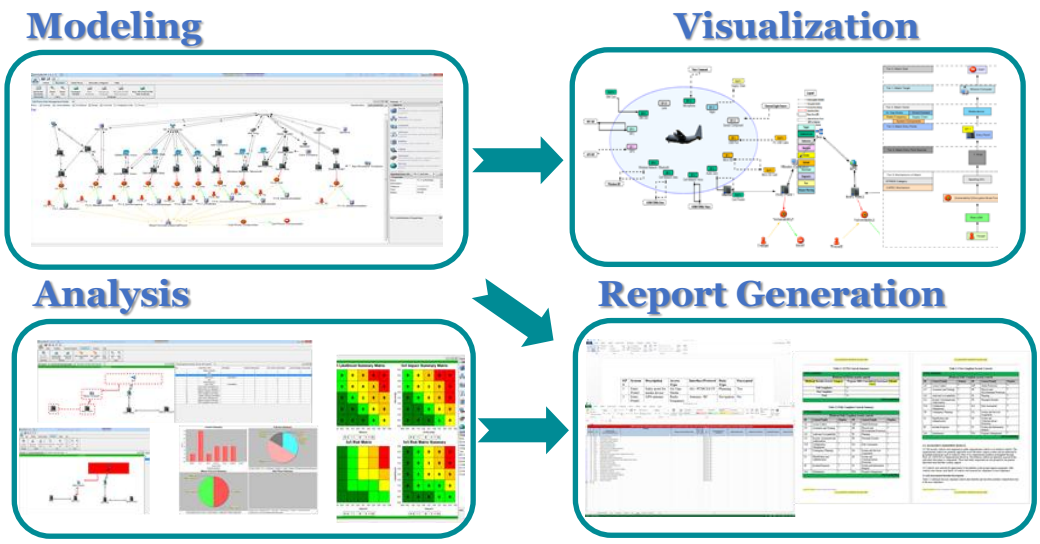
The ASSURANT™ suite is deployed as a modeling, documentation, and analysis layer that helps operators evaluate the way technical controls fit within a broader OT cyber-physical security strategy.

Conclusion and Recommendations

The last decade has shown that OT cybersecurity incidents can produce consequences well beyond data loss. Production interruptions, fuel or supply disruption, safety concerns, environmental consequences, and reputational damage are all realistic outcomes. Digitization and IT-OT convergence have increased both the value and the exposure of refinery systems, making disciplined risk management, incident planning, and architecture assurance more important.[23]

Top recommendations include the following:

- Inventory, model, and document OT systems to improve visibility and support governance.
- Segment networks according to ISA/IEC 62443 principles, Purdue-aligned architecture concepts, and zero-trust design practices where appropriate.[6]
- Continuously assess asset vulnerabilities by correlating inventories with CVEs, KEV catalogs, and threat intelligence. [7][8]



- Plan and exercise incident response scenarios that integrate process safety, IT, and OT decision-making. [9]
- Align internal practices with external standards and participate in sector information-sharing where possible.
- Invest in workforce development and tools that help teams manage architectural complexity more consistently.

KBSI's ASSURANT™ Cyber-Physical Security suite is a platform that can help refinery operators document complex OT environments, analyze dependencies, and support continuous risk-reduction efforts alongside other security and operational controls.

A model-based, defense-in-depth, and evidence-driven approach to OT cybersecurity is increasingly a practical requirement for maintaining safe, reliable, and resilient refinery operations.

Citations

1. National Petroleum Council, "Purdue Model Framework for Industrial Control Systems & Cybersecurity Segmentation," Topic Paper no. 4-14, in Dynamic Delivery—America's Evolving Oil and Natural Gas Transportation Infrastructure (Washington, DC: National Petroleum Council, December 12, 2019), https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf
2. Dragos, "2025 OT/ICS Cybersecurity Report: A Year in Review," 2025, https://hub.dragos.com/ot-cybersecurity-year-in-review-2025
3. Microsoft Threat Intelligence, "Volt Typhoon Targets US Critical Infrastructure with Living-off-the-Land Techniques," Microsoft Security Blog, May 24, 2023, https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.
4. Cybersecurity and Infrastructure Security Agency, "AA21-131A: DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks," July 8, 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a
5. Mandiant, "Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure," Google Cloud Blog, December 14, 2017, https://cloud.google.com/blog/topics/threat-intelligence/attackers-deploy-new-ics-attack-framework-triton.

6. International Society of Automation, "ISA/IEC 62443 Series of Standards," accessed April 21, 2026, https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.
7. Cybersecurity and Infrastructure Security Agency, "Cybersecurity Performance Goals 2.0 (CPG 2.0)," 2025, https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0.
8. SynSaber, "SynSaber Releases ICS CVE Retrospective: 3 Years of CISA Advisories," PR Newswire, February 9, 2023, https://www.prnewswire.com/news-releases/synsaber-releases-ics-cve-retrospective-3-years-of-cisa-advisories-301742812.html.
9. National Institute of Standards and Technology, Guide to Operational Technology (OT) Security, Special Publication 800-82, Rev. 3 (Gaithersburg, MD: National Institute of Standards and Technology, September 2023), https://doi.org/10.6028/NIST.SP.800-82r3.
10. IBM, "X-Force Threat Intelligence Index 2024 Reveals Stolen Credentials as Top Risk, with AI Attacks on the Horizon," 2024, https://www.ibm.com/think/x-force/2024-x-force-threat-intelligence-index.
11. Mandiant, "M-Trends 2024: Our View from the Frontlines," Google Cloud Blog, April 23, 2024, https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2024.

