Safeguarding Industry 4.0
by DTS Solution

Data Sheet

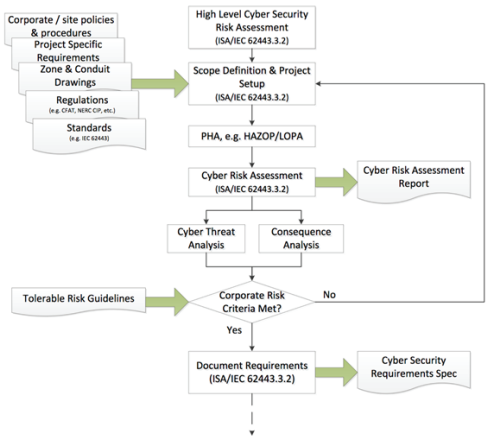
Industrial Cyber Security
Risk Assessment

DTS Solution – ICS / OT Cyber Security consulting services delivers in-depth OT / ICS Cyber Security Assessment across various industry verticals. We have performed OT / ICS and IIoT Cyber Security Assessment across the following industry verticals;

- Petrochemical
- Utilities - Power Generation and Transmission
- Oil & Gas
- Refinery
- Airport
- Manufacturing
- Smart City

Our methodology for conducting the OT / ICS Cyber Security Assessment is based on the following project phases;

- Project Planning
- Risk Management Methodology and Enterprise Rating Context
- OT Cyber Security Assessment - CSMS Review
- OT Cyber Security Assessment - Technical Review
- OT Cyber Security Assessment Reporting
- OT Cyber Security - Development Phase (Optional)

SL.	Project Phase	Description - ICS/OT Cyber Security Risk Assessment
0	Project Planning	Preparation of the project execution plan and project management services
1	Risk Management Methodology and Enterprise Rating Context	Analysis of business and industrial facility context, enterprise risk appetite for industrial failure due to cyber risk, and cyber risk management practices adopted within OT i.e. task risk assessment methodology using Cyber PHA / HAZOP methodologies. Review existing risk management practices to rate risks based on safety integrity levels, security assurance levels and hazard levels and for it to be adopted to perform cyber risk assessment and quantifying risks. Ensure the organization's Enterprise Risk Management (ERM) process requirements and metrics are aligned to industrial operations and the selected risk methodology and rating are in line with organization's ERM process that are aligned with QHSE and OT operations. This risk management methodology will then be adopted to perform technical security assessment and review in subsequent project activities. 

SL.	Project Phase	Description - ICS/OT Cyber Security Risk Assessment
2	OT Cyber Security Assessment – CSMS Review	Analysis of industrial processes and available documentation (CSMS) • ICS Security Policies • ICS Security Processes • ICS Security Procedures • ICS Security Operating Manual • ICS Asset Management • ICS Incident Response Plan • ICS Security Architecture Blueprint • ICS Security – Workforce Development • ICS Security – Risk Management Framework
		Analysis of ICS security objectives and ICS operating model
		Analysis of existing ICS security design and practices
		Analysis of technical documentation (systems description, process & safety control schemes, network diagrams.) Review of the Functional Design Specification (FDS) Review of the Detailed Design Specification (DDS)
3	OT Cyber Security Assessment – Technical Review	Providing comprehensive engineering and consultancy services for the following cyber risk assessment for the OT environment: TECHNICL ARCHITECTURE AND REFERENCE MAPPING • ICS security requirements specification Security Design and Architecture Review – Network Architecture and Topology Review • Security Zoning and Conduit Architecture • Industrial Control Systems Security Assurance and Framework (NIST CSF v1.1) Gap Assessment TECHNICL SECURITY ASSESSMENT • Technical Plant Control Systems Security Assessment (Packages) o BPCS o PIN o ESD o F&G o PMS o APC o Vibration Monitoring System • Safety Instrumented Systems (SIS) and Field Devices Security o PLC, RTU, IED • Network Security, Anomaly Detection, and Endpoint Protection Infrastructure Assessment and OT Application Assessment • Industrial Wireless Assessment and Physical Security Assessment • Industrial Protocol Security Analysis (analysis of PCAP files from critical network segments) • Technical review of backup and recovery controls • Technical review of ICS security visibility – logging and monitoring controls against MITRE ICS ATT&CK Model • Review of Cyber Security Practices; o Patch Management o Hardening Practices o Obsolescence Management o Account Review and Authorization o Use of Removable Media o Change Management o Backup o Availability Monitoring o Logging and Monitoring (OT CSOC) o Threat Intelligence o 3rd Party Remote Access o Application Whitelisting o Endpoint Security
		Review current ICS system asset inventory and perform a gap assessment on its current state
		Study and propose a secure mechanism for remote access case by case after analyzing that the access requirement and ensure the access will not introduce threat vector to the organization's ICS environment i.e. IT and OT connectivity, DCS OEM vendor remote diagnostic services, on-demand remote support etc
		Perform a detailed comprehensive penetration test from IT network with the objective of obtaining access into the OT environment. Securing the IT and OT connectivity. Perform a security architecture review of the IT and OT connectivity including traffic flow, firewall policy review, systems security review.

SL.	Project Phase	Description - ICS/OT Cyber Security Risk Assessment
4	OT Cyber Security Assessment – Reporting	Develop detailed cyber security assessment report based on the various assessments performed during deliverable 3. The detailed risk assessment report will quantify corporate enterprise risk metrics based on threat analysis and consequence analysis as outlined by the levels in deliverable 1.
5	OT Cyber Security – Development Phase (OPTIONAL)	Preparation of model architecture and security target, capabilities and maturity levels will be documented that also satisfy compliance requirements such as ISA S99/IEC 62443 and gaps identified in previous audit reports based on; 1. Target security levels (SL-T) 2. Capability security levels (SL-C) 3. Achieved security levels (SL-A) Security Capabilities level identified based on the model architecture 1. FR1 – Identification and Authentication Control 2. FR2 – Use Control 3. FR3 - System Integrity 4. FR4 – Data Confidentiality 5. FR5 – Restricted Data Flow 6. FR6 – Timely Response to Events 7. FR7 – Resource Availability Current maturity levels vs. target maturity levels.
		Development of security implementation roadmap and strategy
		Development of RFP Package, bill of materials and vendor selection criteria for security enhancement and hardening.
		Development a procedure of implementation an Intrusion Detection System (IDS) / solution at the ICS process networks to detect possible intrusions from the OT network, in consultation with the ICS vendors for the various systems employed by the organization. Development of Cyber Threat Intelligence Procedure for ICS targeted malware.
		Development of mechanism to self-check (health-check) the ICS cyber security compliance with security standards or guidelines – daily, weekly and monthly health-checklist