The Industrial Control System
Cybersecurity Lifecycle

exida

	INPUT	PROCESS	OUTPUT	exida services

Assess Phase

INPUT:
- Corporate / site policies and procedures
- Project Specific Requirements
- Architecture Drawing(s)
- Regulations (e.g. NERC CIP, CFATS, etc.)
- Standards (e.g. ISA/IEC 62443.3.3)

- HAZOP & SIL Selection
- Cybersecurity Risk Assessment Procedure
- Knowledge of process and business impact

- Tolerable Risk Guidelines

- Standards (e.g. ISA/IEC 62443.3.2)
- Reference Architectures & Best Practices

PROCESS:
- Scope Definition and Project Setup (ISA/IEC 62443.3.2)
- Cybersecurity Vulnerability Assessment
- Cybersecurity Risk Assessment (ISA/IEC 62443.3.2)
- Cybersecurity Target Selection (ISA/IEC 62443.3.2)
- Zone and Conduit Model (ISA/IEC 62443.3.2)
- Document Requirements (ISA/IEC 62443.3.2)

OUTPUT:
- Project Management Plan
- Cybersecurity Vulnerability Assessment Report
- Cybersecurity Risk Assessment Report
- Zone and Conduit Drawing(s)
- Cybersecurity Requirements Specification (CRS)

exida services:
- Analyze and create existing architecture drawing(s)
- Policy development and/or review
- Cybersecurity Awareness Training

- Perform Cybersecurity Vulnerability Assessment
- Update Architecture Drawing(s)
- Evaluation of existing countermeasures
- Windows Security Vulnerability Assessment (WSVA)
- Cybersecurity Scorecard
- Development of cybersecurity risk assessment procedure
- Train staff on risk assessment procedure
- Facilitate and Document Risk Assessment
- Threat Modeling

- Facilitate Cybersecurity Target Selection

- Zone and Conduit Modeling
  - Development of corporate reference models
  - High-level diagrams
  - Detailed design
  - Design reviews

- Cybersecurity Requirements Specification (CRS) Template
- CRS Development
- CRS Review

Implement Phase

INPUT:
- Cybersecurity Requirements Specification (CRS)
- Cybersecurity Design Spec (CDS)
- Cybersecurity Requirements Specification (CRS)
- Security Manuals of ICS Products
- Design Package (Drawings, Configurations, Procedures)
- Cybersecurity Factory Acceptance Test (CFAT) Plan
- Cybersecurity Site Acceptance Test (CSAT) Plan

PROCESS:
- Conceptual Design (ISA/IEC 62443.3.2)
- Design Validation (ISA/IEC 62443.3.2)
- Adequate Design? — NO
- Detailed Design
- Develop Test Plans (ISA/IEC 62443.3.2)
- Implement Design
- Cybersecurity Factory Acceptance Test (CFAT) (ISA/IEC 62443.2.4)
- Installation/ Commissioning (ISA/IEC 62443.2.4)
- Cybersecurity Site Acceptance Test (CSAT) (ISA/IEC 62443.2.4)

OUTPUT:
- Cybersecurity Design Spec (CDS)
- Validation Report
- Design Package (Drawings, Configurations, Procedures)
- Cybersecurity Factory Acceptance Test (CFAT) Plan
- Cybersecurity Site Acceptance Test (CSAT) Plan
- Cybersecurity Factory Acceptance Test (CFAT) Report
- CSAT Test Report

exida services:
- Cybersecurity Design Specification (CDS) Consultation
- CDS Review
- Technology Investigation

- Defense-in-Depth Analysis (analysis of effectiveness of defense layers)
- Detection-in-Depth Analysis (analysis of effectiveness of monitoring layers)

- Development of Procedures
- ACL Development/Review
- Design Reviews

- Cybersecurity Factory Acceptance Test (CFAT) Plan Development
- Cybersecurity Site Acceptance Test (CSAT) Plan Development
- Test plan review

- Cybersecurity Factory Acceptance Testing (CFAT)
- Windows Cybersecurity Vulnerability Assessment (WCVA)

- Cybersecurity Site Acceptance Test (CSAT)
- Windows Cybersecurity Vulnerability Assessment (WCVA)

Maintain Phase

INPUT:
- Patch Management Procedure
- Antivirus Management Procedure
- Security Monitoring Procedure
- Change Management Procedure
- ICS Cybersecurity Assessment Procedure

PROCESS:
- Countermeasure Maintenance
- Security Monitoring
- Modifications or Decommision
- Modifications? — YES → To appropriate lifecycle phase
- Periodic Assessment

OUTPUT:
- Maintenance Records
- System Logs (IDS / SIEM)
- Impact Analysis
- Change Request
- ICS Cybersecurity Assessment Report

exida services:
- Vulnerability Management Service

- Develop logging requirements
- Design monitoring methods
- Review

- Impact Analysis Review

- Perform ICS Cybersecurity Assessment
- Windows Cybersecurity Vulnerability Assessment (WCVA)
- Cybersecurity Scorecard

Control System Security Management Program: Policy, Standards, Procedures, Training, Awareness
(ISA/IEC62443.2.1 formerly ISA99.02.01)

www.exida.com/security
security@exida.com