Security Brief

Practical guidelines for conducting IEC 62443 assessments using Radiflow products

The Radiflow Cyber-research team

radiflow

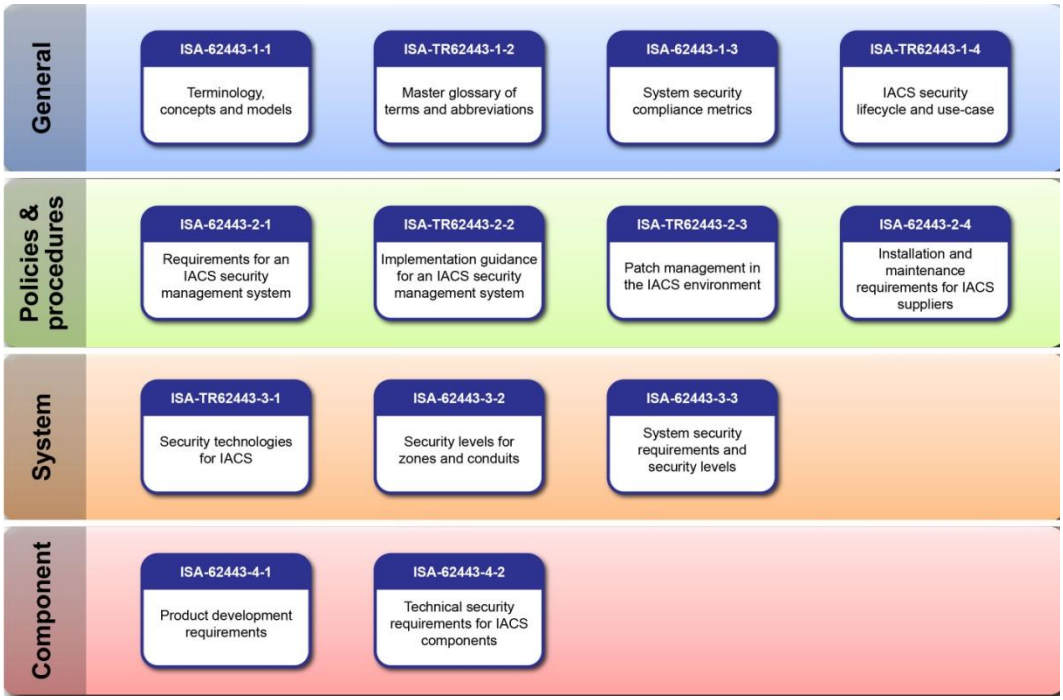
PRACTICAL GUIDELINES FOR CONDUCTING ISA/IEC 62443 ASSESSMENTS USING RADIFLOW PRODUCTS

The increasing cyber threats and vulnerabilities in industrial control system (ICS) networks can affect the availability of the industrial environment and cause significant damage to manufacturing enterprises. ISA/IEC 62443 (formerly known as ISA 99) helps organizations to reduce both the risk of failure and the exposure of ICS networks to cyber threats. Aligning with the standard is important to protect critical control systems and indeed it has been adopted by many firms in the industrial sector.

The goal of this white paper is to provide a simple and practical guide for conducting ISA/IEC 62443 assessments using Radiflow products. It describes how performing a risk assessment process can help protect your network by identifying critical business processes, prioritizing the risk scenarios jeopardizing these business processes and taking effective countermeasures to mitigate these risks. All of the steps described are compliant with ISA/IEC 62443 and accompanied by examples taken from a risk assessment report performed by our ICS lab.

INTRODUCTION TO IEC 62443

ISA/IEC 62443 is the global standard for securing Industrial Automation and Control Systems (IACS) networks. It helps organizations to reduce both the risk of system failure and the exposure to cyber threats. ISA/IEC 62443 consists of 14 documents divided into four groups: General, Policies and Procedures, System and Component.



The different sections and sub-topics of the IEC-62443 standard

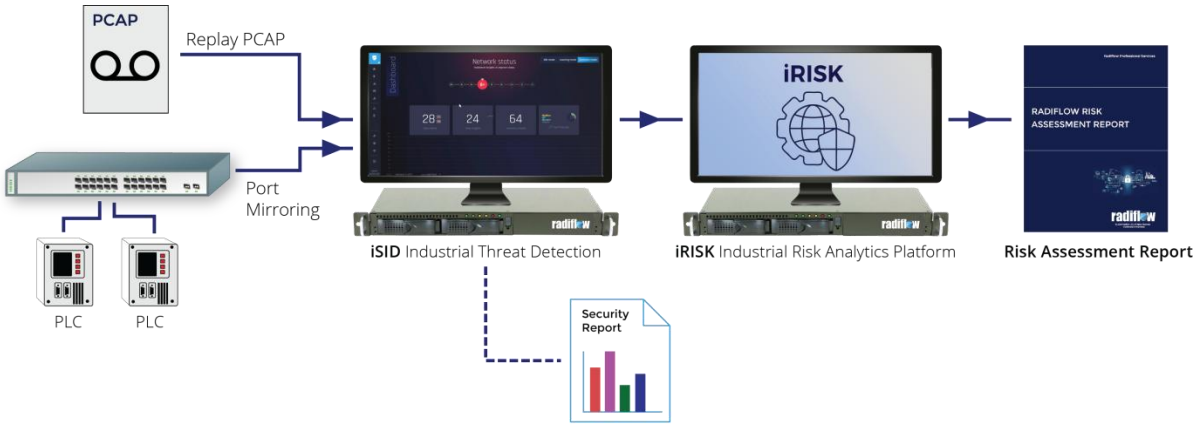
COMPLIANCE VIA RADIFLOW'S ISID AND CIARA

The iSID Industrial Threat Detection and Analysis System and the CIARA Business-Driven Risk Assessment System provide the user with visibility into the industrial network and ICS assets, including prioritization of the top business processes at the facility and top ICS risks per business process.

More information about iSID and CIARA is available on the Radiflow website.

PROCESS

1. **Monitor**: iSID monitors the network by conducting port mirroring on the customer's OT network. In addition, the user can replay a PCAP file containing network traffic data using iSID's "traffic replay" feature.
2. **Export**: iSID's analysis results, including all the identified assets, links, business processes, criticality and events detected in the network, is exported to CIARA to be used as input for risk calculation.
3. **Calculate**: CIARA's algorithm simulates the likelihood that a threat to an asset or business process would materialize using the MITRE ATT&CK methodology, based on multiple variables including interplay between business processes and assets, historical IT/OT protocol data and open-source vulnerability notices (CVSSs). This provides an accurate assessment of the risk to specific business processes and to the entire production network.
4. **Report**: at the end of the process CIARA produces a graphical risk assessment report detailing all network assets, business processes, topology and vulnerability, as well as detailed risk-based recommendations and actionable mitigation roadmap to reduce network risk.



IEC-62443 COMPLIANCE BY FEATURE/CAPABILITY

RADIFLOW AS COMPLIANCE ENABLER FOR IEC-62443 BY SECTION

62443-1-1 3.2.88:	Conducts a Risk assessment process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources; quantifies loss exposures and consequences based on probability
62443-1-1 5.11, 6.5.4:	Map Zones and business processes and the Security level targets for each
62443-2-1:	Define your Business Rationale (based on the nature and magnitude of financial, HSE, and other potential consequences should IACS cyber incidents occur.)
62243-2-1 4.2.3.12:	Conduct risk assessments throughout the lifecycle of the IACS
62243-2-1 4.2.3.14:	Maintain vulnerability assessment records
62443-2-1 A.2.2, A.2.3:	Automated Risk and Vulnerability assessment report using baseline and attack scenarios
62443-2-3 B.3.1:	Inventory of existing network architecture and connectivity
62443-2-3 B.3.5:	Evaluation and assessment of existing environment
62443-2-3 B.8.3, C.2.1:	Discovery and identification of the security vulnerabilities in IACS as a basis for the patch management process
62443-2-3 B.6.8:	Risk mitigation alternatives
62443-2-3 B.7.5, B.8.2:	Change management audit verifying that the patch was installed per target device and the vulnerability has been mitigated
62443-3-3:	Mapping of deployed SRs and Recommendation & Prioritization of mitigations for these SRs

ISID: BUSINESS PROCESS IDENTIFICATION

Assets in iSID are associated to business processes. The user can edit asset groupings by adding, removing or moving assets from one business process to another according to the factory operations. The user can also assign a unique name for each business process to describe its functionality.

ISID: CLASSIFICATION OF BUSINESS PROCESSES CRITICALITY

iSID assigns a default criticality value to different business processes it detects (based on function). This value can be changed by the user, based on the estimated impact of each business process's loss of availability on the organization as a whole. Options are HSE (Health Safety Environmental), Major impact, Minor impact and others.

- ***Compliant with IEC 62443-2-1****: "Define your Business Rationale (based on the nature and magnitude of financial, HSE, and other potential consequences should IACS cyber incidents occur.)"*

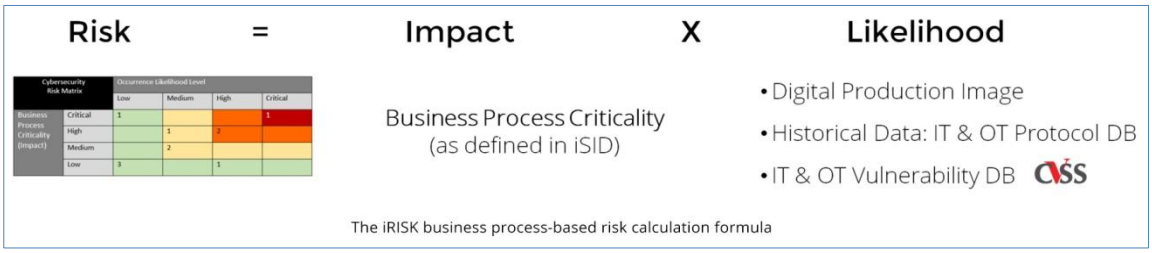
CIARA: BUSINESS PROCESS-BASED RISK CALCULATION

CIARA calculates the risk for each detected business process according to its criticality (severe or minor business impact, HSE or other) and likelihood (low to critical) of being attacked.

Cybersecurity Risk Matrix		Occurrence Likelihood Level			
		Low	Medium	High	Critical
Business Process Criticality (Impact)	Critical	1			1
	High		1	2	
	Medium		2		
	Low	3		1	

One of the crucial elements in detecting and mitigating risk is identifying devices on critical paths (i.e. connected to multiple critical devices), as they are more likely to be compromised. Securing devices on critical paths reduce significantly risk.

CIARA displays the number of business processes at different risk levels (color-coded from green to red) taking into account the criticality of the business process (based on the impact a disturbance would have on the organization) and the likelihood of an attack on devices connected to that business process.



The iRISK business process-based risk calculation formula

- ***Compliant with 62443-2-1****: Define your Business Rationale (based on the nature and magnitude of financial, HSE, and other potential consequences should IACS cyber incidents occur.)*

CIARA RISK SCENARIO DETECTION AND PRIORITIZATION

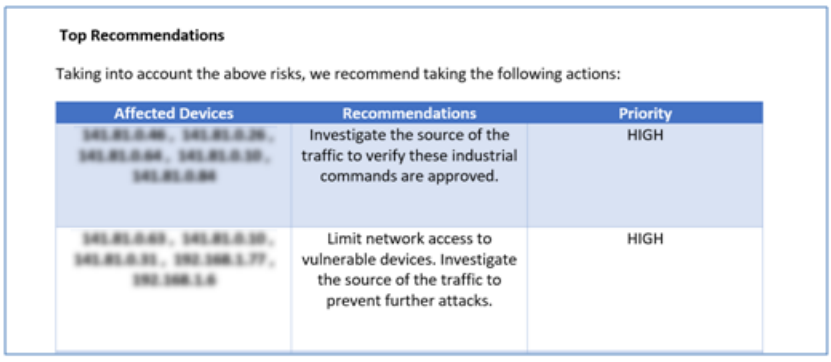
CIARA calculates a risk score for each risk scenario detected by iSID based on the scenario's impact on the affected business process and its assets. The risk scenarios are sorted, prioritized and presented to the user, towards optimizing risk mitigation and provisioning expenditure.

Risk Description	Category	Risk
Modbus diagnostic command sent to PLC in a critical business process (pumping water) from an unauthorized user	Cyber Attack	High
Unauthorized DNP3 Write Request sent to a critical business process with high availability requirements	Cyber Attack	High
Cold restart DNP3 command sent from unauthorized client	Cyber Attack	High
Siemens invalid command to a PLC from a new detected server	Cyber Attack	High
ICS assets which send DNS requests to the internet	Assets	High
Modicon PLC with old firmware	Assets	Medium
Operational anomaly - assets are changing the configuration of other assets in the network	Cyber Attack	Medium
SCADA server with 10 open ports	Assets	Low

- ***Compliant with 62443-1-1 3.2.88****: Risk assessment process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources; quantifies loss exposures and consequences based on probability*

CIARA: RECOMMENDATIONS AND RISK-MITIGATION MEASURES

CIARA's assessment report provides a complete actionable remediation plan for reducing the network's overall risk score based on Sectorial and Geo-location Threat Intelligence, risk scenarios, asset vulnerabilities and the analyzed network topology.



Top Recommendations

Taking into account the above risks, we recommend taking the following actions:

Affected Devices	Recommendations	Priority
[redacted]	Investigate the source of the traffic to verify these industrial commands are approved.	HIGH
[redacted]	Limit network access to vulnerable devices. Investigate the source of the traffic to prevent further attacks.	HIGH

- ***Compliant with the*** **ISA/IEC 62443** requirement for Mitigation Recommendation & Prioritization

CIARA: DETECTION OF THREATS AND VULNERABILITIES

CIARA displays relevant network vulnerabilities, as detected (passively) by iSID, in a clear tabulated format. Vulnerabilities are ranked and sorted by their CVSS V3 scores. In addition CIARA displays the top exploitable vulnerabilities and the newest vulnerabilities in the network.

CVSSv3 Score	CVE-ID	Vulnerability	IPs	Exploitable
9.8 High	CVE-2020-6967	Remote code execution in Rockwell Automation FactoryTalk Diagnostics	10.0.0.8, 10.1.1.165, 141.81.0.104 141.81.0.130 141.81.0.144	Yes

- ***Compliant with*** *IEC 62443-2-1 A.2.3.3.2: Automated Risk and Vulnerability assessment report; and IEC 62443-1-1 3.2.88 & 62443-3-3: Risk assessment process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources; quantify loss exposures and consequences based on probability.*

CONCLUSION

iSID's business processes detection capabilities, combined with CIARA's unique risk calculation algorithm, provide compliance with the sections in ISA/IEC 62443 CSMS regarding risk assessment:

- **62443-1-1 3.2.88**: Risk assessment process for vulnerabilities with quantitative calculation of consequences based on probability
- **62443-1-1 5.11, 6.5.4**: Map Zones and business processes and the Security level targets for each
- **62443-2-1**: Definition of Business Rationale
- **62243-2-1 4.2.3.12**: Risk assessments throughout the lifecycle of the IACS
- **62243-2-1 4.2.3.14**: Maintain vulnerability assessment records
- **62443-2-1 A.2.2, A.2.3**: Automated Risk and Vulnerability assessment report
- **62443-2-3 B.3.1**: Inventory of existing network architecture and connectivity
- **62443-2-3 B.3.5**: Evaluation and assessment of existing environment
- **62443-2-3 B.8.3, C.2.1**: Discovery and identification of the security vulnerabilities in IACS
- **62443-2-3 B.6.8**: Risk mitigation alternatives
- **62443-2-3 B.7.5, B.8.2**: Change management audit
- **62443-3-3**: Mapping of deployed SRs as well as mitigation recommendations for these SRs

ABOUT RADIFLOW

Radiflow is a leading provider of industrial cyber security solutions for critical business operations. Our comprehensive portfolio of cybersecurity solutions empowers critical infrastructure and industrial enterprises to maintain visibility, control and security of their operational environment. Our intelligent threat management for Industrial cybersecurity minimizes potential business interruption and loss within your OT environment. The Radiflow team consists of professionals from diverse backgrounds, from veterans of military cyber and communications units to former employees of leading players in the industry. Founded in 2009, Radiflow' first solutions were launched in late 2011, validated by leading research labs and successfully deployed by major utilities worldwide. More at www.radiflow.com.