

# Securing Critical Infrastructure Worldwide with IEC 62443

The World’s Only Consensus-Based OT Cybersecurity Standards

## ISA/IEC 62443: A Universal Framework

COUNTRIES ADOPTING ISA/IEC 62443 AROUND THE GLOBE

INTERNATIONAL ENDORSEMENTS



## The ISA/IEC 62443 Framework

4 groups | 16+ Documents | 20+ Years of Industry-Driven Evolution

GROUP 1: GENERAL Foundation & Terminology	GROUP 2: POLICIES AND PROCEDURES Security Programs	GROUP 3: SYSTEM System-Level Requirements	GROUP 4: COMPONENT Product Requirements
<ul style="list-style-type: none"><li>Common concepts, models, metrics</li><li>Lifecycle use cases</li><li>IIoT considerations</li></ul>	<ul style="list-style-type: none"><li>Establishing IACS security programs</li><li>Service provider requirements</li><li>Patch management guidance</li></ul>	<ul style="list-style-type: none"><li>Security technologies</li><li>Risk assessment methodologies</li><li>Security requirements by level</li></ul>	<ul style="list-style-type: none"><li>Secure development lifecycle</li><li>Technical component requirements</li><li>Embedded devices to applications</li></ul>

## Industries Secured by ISA/IEC 62443

Horizontal Standard = Universal Application

<b>Manufacturing</b> Discrete and Process Manufacturing	<b>Electric Grid</b> Generation and Distribution	<b>Oil and Gas</b> Upstream, Midstream and Downstream	<b>Water Systems</b> Treatment and Distribution	<b>Transportation</b> Rail, Pipeline, Ports
<b>Healthcare</b> Medical Device Manufacturing	<b>Building Automation</b> Critical Facility Systems	<b>Chemical</b> Process Industries	<b>Pharmaceuticals</b> Production Facilities	<b>Mining</b> Operations and Processing

## Key Benefits of ISA/IEC 62443

Why Organizations Choose ISA/IEC 62443

<b>RISK-BASED APPROACH</b> Security tailored to your unique threat landscape	<b>COMMON LANGUAGE</b> Unified terminology for asset owners, suppliers, service providers	<b>LIFECYCLE SECURITY</b> Protection from design through decommissioning
<b>REDUCED COSTS</b> Standards-based efficiency reduces overall lifecycle expenses	<b>REGULATORY ALIGNMENT</b> Referenced in global frameworks and emerging regulations	<b>TECHNOLOGY NEUTRAL</b> Functional objectives, not prescriptive solutions

## How Dragos Aligns with ISA/IEC 62443

The Dragos Platform: Automated Visibility and Threat Detection

<b>SR 1.13 MONITOR/CONTROL NETWORK ACCESS</b> Continuous monitoring of all OT access points	<b>SR 2.8 GENERATE SECURITY AUDIT RECORDS</b> Comprehensive logging across access control, system events, configuration changes	<b>SR 6.2 CONTINUOUS SECURITY MONITORING</b> Purpose-built IDS for industrial protocols & OT behaviors
<b>SR 7.8 REPORT INSTALLED COMPONENTS</b> Automated, continuously updated asset inventory with firmware versions	<b>SR 3.2 MALICIOUS CODE PROTECTION</b> Detection of malware, unauthorized software, suspicious behaviors	<b>SR 5.2 ZONE BOUNDARY MONITORING</b> Monitor/control communications at security boundaries

Professional Services: Risk-Based Program Development

<b>ZCR 2.1 HIGH-LEVEL CYBERSECURITY RISK ASSESSMENT</b> Industry-specific experts conduct comprehensive risk evaluations	<b>DRAR 12 DOCUMENT RISK ASSESSMENT RESULTS</b> Architecture diagrams, vulnerability assessments, actionable roadmaps	<b>SR 5.1 LOGICAL NETWORK SEGMENTATION</b> Zone and conduit model development with defensible architectures	<b>ZCR 3.1 ESTABLISH ZONES AND CONDUITS</b> Asset grouping based on criticality, function, risk profiles
-----------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------

Threat intelligence: Understanding Real-World OT Adversaries

<b>SR 3.2 PREVENT/DETECT/MITIGATE MALICIOUS CODE</b> Detection TTPs for known OT adversary campaigns	<b>DRAR 1 LIST THREATS AFFECTING ASSETS</b> Threat source descriptions, vectors, affected asset identification	<b>DRAR 2 DOCUMENT KNOWN VULNERABILITIES</b> Practical, prioritized vulnerability mitigation advice	<b>ZCR 5.4 DESCRIBE THREAT ENVIRONMENT</b> Current and emerging threat intelligence for OT environments
---------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------

## Ready to Align with IEC 62443?

Download our solution brief to see detailed mapping of Dragos capabilities to specific standards requirements.