# 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** 



**National Adoption** 

**INTERNATIONAL ENDORSEMENTS** 



**United Nations** 



IEC Designated "Horizontal Standard"



Cybersecurity Framework



Cybersecurity Performance Goals



**EU** Regulatory Framework (NIS2, CRA)

# The ISA/IEC 62443 Framework

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



### **GROUP 1: GENERAL Foundation & Terminology**

models, metrics

• Common concepts,

- Lifecycle use cases
- IIoT considerations



### **AND PROCEDURES Security Programs**

• Establishing IACS

security programs

- Service provider requirements
- Patch management guidance



### **System-Level** Requirements

Security

Risk assessment

methodologies

technologies

- Security requirements by level
- **GROUP 4: COMPONENT**



**Product Requirements** 

- - component requirements

Technical

• Embedded devices to applications

# Industries Secured by ISA/IEC 62443

Horizontal Standard = Universal Application



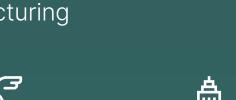
**Manufacturing** Discrete and Process

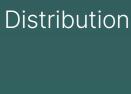
Manufacturing

**Healthcare** 

Medical Device

Manufacturing





**Electric Grid** 

Generation and

**Building** 

**Automation** 

Critical Facility

Systems



Midstream and Downstream



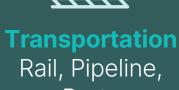
**Process** 

Industries





**Pharmaceuticals** 









**Mining** 

Operations and

Processing

# Key Benefits of ISA/IEC 62443 Why Organizations Choose ISA/IEC 62443

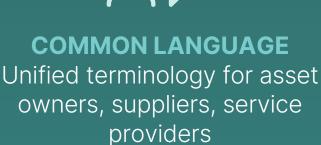


**REDUCED COSTS** 

Standards-based efficiency

reduces overall lifecycle

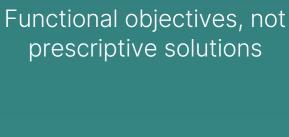
expenses







**TECHNOLOGY NEUTRAL** 



# How Dragos Aligns with ISA/IEC 62443 The Dragos Platform: Automated Visibility and Threat Detection

**NETWORK ACCESS AUDIT RECORDS SECURITY MONITORING** Comprehensive logging across Purpose-built IDS for industrial Continuous monitoring of all OT access points access control, system events, protocols & OT behaviors

**SR 2.8 GENERATE SECURITY** 

### **SR 7.8 REPORT INSTALLED**

**SR 1.13 MONITOR/CONTROL** 

**COMPONENTS** 

Automated, continuously updated asset inventory with firmware versions

## **SR 3.2 MALICIOUS CODE**

**PROTECTION** 

configuration changes

Detection of malware, unauthorized software, suspicious behaviors

## **SR 5.2 ZONE BOUNDARY**

**MONITORING** 

boundaries

Monitor/control communications at security

**SR 6.2 CONTINUOUS** 

Professional Services: Risk-Based Program Development

### **RESULTS SEGMENTATION CONDUITS RISK ASSESSMENT** Architecture Zone and conduit Asset grouping based

### experts conduct comprehensive risk evaluations

**ZCR 2.1 HIGH-LEVEL** 

**CYBERSECURITY** 

Industry-specific

## assessments,

**DRAR 12 DOCUMENT** 

**RISK ASSESSMENT** 

actionable roadmaps

### diagrams, vulnerability model development

with defensible architectures

risk profiles

**ZCR 3.1 ESTABLISH** 

on criticality, function,

**ZONES AND** 

Threat intelligence: Understanding Real-World OT Adversaries

### **DRAR 2 DOCUMENT**

Ready to Align with IEC 62443?

### **DETECT/MITIGATE MALICIOUS CODE Detection TTPs for** known OT adversary

**SR 3.2 PREVENT/** 

campaigns

# **DRAR1LIST**

affected asset

identification

**THREATS AFFECTING ASSETS** Threat source descriptions, vectors,

### **KNOWN VULNERABILITIES**

**SR 5.1 LOGICAL** 

**NETWORK** 

Practical, prioritized vulnerability mitigation advice

### **ZCR 5.4 DESCRIBE THREAT ENVIRONMENT** Current and emerging

threat intelligence for

OT environments

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