Applying IEC 62443-4-1 to Industrial Automation Control Systems

Security for Industrial Automation and Control Systems (IACS)

www.ldra.com

* Registration required to download the document

Introduction

Automated control systems are nothing new. As long ago as the late 1950s, the third industrial revolution (or digital revolution) saw the beginnings of a trend away from purely mechanical and analogue electronic technologies towards an integration with information technology, and the ever-increasing complexity of industrial systems soon resulted in demands for improved levels of safety. To meet this demand, functional safety standards were written to provide guidance in the development of systems that are either fail safe, or that fail in a predictable manner. In 1998, the International Electrotechnical Commission (IEC) published IEC 61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems", a universal functional safety standard applicable to all kind of industry. Updated in 2010, IEC 61508 is underpinned by two fundamental principles - a "safety lifecycle" development process that aims to eliminate design errors by leveraging best practices, and a probabilistic failure approach that accounts for the safety impact of device failures.

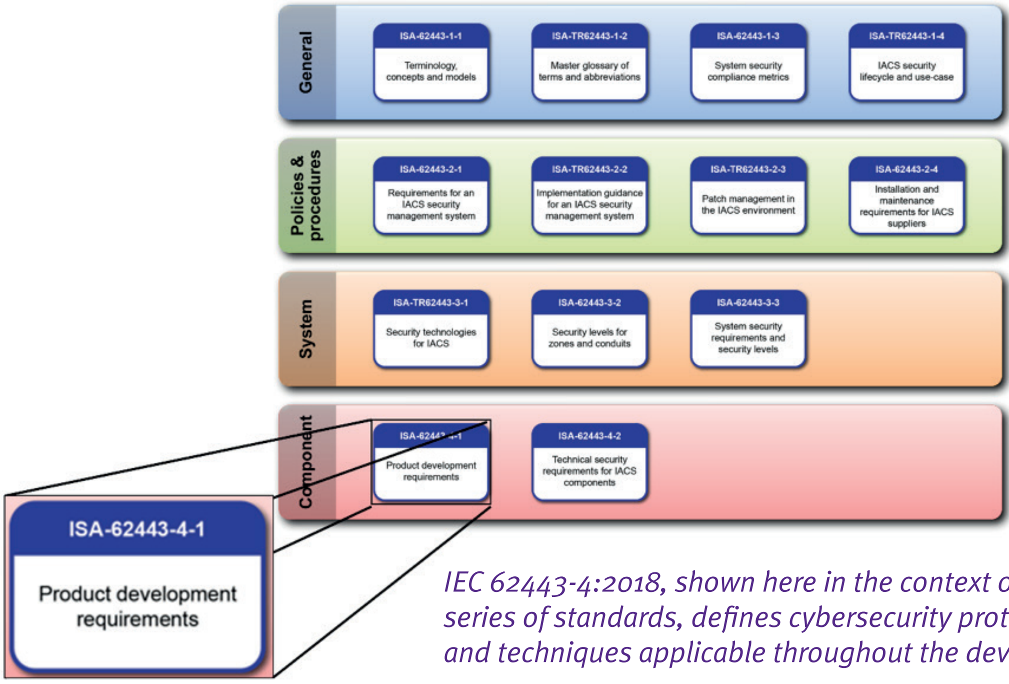
Building upon these established technologies and principles, the "fourth industrial revolution" concerns the seismic impact that the addition of cyber-physical systems, the Internet of Things, and the Internet of Systems has on the way we live, work and relate to each other. Such changes clearly have implications for manufacturing, process, and a host of other industries. "Industrie 4.0" (or Industry 4.0, or I40), a national strategic initiative from the German government, is a prominent example of how industry is addressing the resulting constraints and challenges.

Inside smart factories, cyber-physical systems (CPS) have to be synchronized each other and with the external world to share information and trigger actions. This cyber-physical connectivity and the associated challenges of ensuring secure development, deployment and operation of systems are fundamental to Industrie 4.0, with networked embedded systems ranging from domestic audio/video systems to supervisory control and data acquisition (SCADA) systems controlling entire production plants.

In general, there is far more public awareness of the dangers of cyberattack (viruses, worms and malware) upon personal computers than these networked devices and infrastructure they have come to rely on. Systems therefore need to be impervious to attack without relying on the user "doing the right thing" to protect them, and it is the remit of the IEC to set the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure. Their ISA99 committee together with the IEC Technical Committee 65 Working Group 10 (TC65WG10) have created the 62443 series of standards to address this need to design cybersecurity, robustness, and resilience into industrial automation control systems (IACS).

Role of IEC 62443 series

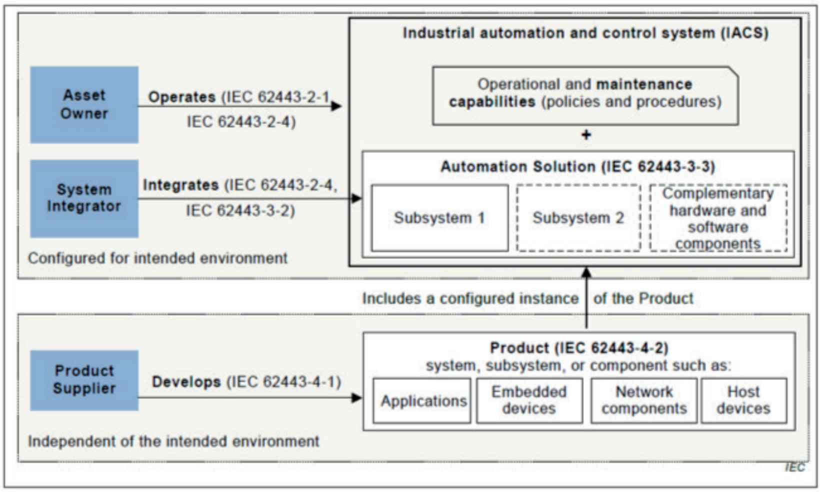
IEC 62443 is a series of multi-industry standards defining cybersecurity protection methods and techniques categorised to apply to all stakeholders including manufacturers, asset owners and suppliers. The fourth in the series, IEC 62443-4:2018, specifies the requirements for the secure development of systems used in industrial control and automation. It defines secure development life-cycle requirements related to cybersecurity for products intended for use in the IACS environment and provides guidance on how to meet the requirements described for each element. The development life-cycle phases include security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life. These activities and tasks can be applied to new or existing processes for developing, maintaining, and retiring hardware, software, or firmware.


General
ISA-62443-1-1
Terminology, concepts and models
ISA-TR62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
System security compliance metrics
ISA-TR62443-1-4
IACS security lifecycle and use-case
Policies & procedures
ISA-62443-2-1
Requirements for an IACS security management system
ISA-TR62443-2-2
Implementation guidance for an IACS security management system
ISA-TR62443-2-3
Patch management in the IACS environment
ISA-62443-2-4
Installation and maintenance requirements for IACS suppliers
System
ISA-TR62443-3-1
Security technologies for IACS
ISA-62443-3-2
Security levels for zones and conduits
ISA-62443-3-3
System security requirements and security levels
Component
ISA-62443-4-1
Product development requirements
ISA-62443-4-2
Technical security requirements for IACS components
ISA-62443-4-1
Product development requirements

IEC 62443-4:2018, shown here in the context of the IEC-62443 series of standards, defines cybersecurity protection methods and techniques applicable throughout the development lifecycle.

Application of the guidelines for IACS

The scope of IEC 62443-4-1 is limited to the developer and maintainer of a secure product for use in an IACS environment. The standard encourages security concerns to be proactively addressed at an early stage in the product lifecycle. The figure below shows how resulting dependable, trustworthy and resilient products complement other IACS subsystems.


Industrial automation and control system (IACS)
Asset Owner
Operates (IEC 62443-2-1, IEC 62443-2-4)
Operational and maintenance capabilities (policies and procedures)
+
System Integrator
Integrates (IEC 62443-2-4, IEC 62443-3-2)
Automation Solution (IEC 62443-3-3)
Subsystem 1
Subsystem 2
Complementary hardware and software components
Configured for intended environment
Includes a configured instance of the Product
Product Supplier
Develops (IEC 62443-4-1)
Product (IEC 62443-4-2)
system, subsystem, or component such as:
Applications
Embedded devices
Network components
Host devices
Independent of the intended environment
IEC

8 IEC 62443-4-1 Practices

- ✓ Security management
- ✓ Specification of security requirements
- ✓ Secure by design
- ✓ Secure Implementation
- ✓ Security verification and validation testing
- ✓ Management of security related issues
- ✓ Security update management
- ✓ Security guidelines

- **Specification of security requirements** – Minimum security requirements for the development and deployment of the product must be established, so that there is a common understanding between end-users and product manufacturers of their respective responsibilities. Threat analysis and risk assessment play import roles in identifying and classifying the potential security risks, and they involve the definition of trust boundaries for process, data and control flow including any communication to internal and external peripherals. Mitigation for the risks identified by these processes become part of the system's technical security requirements.

- **Secure by design** – The product need to be designed to implement the security principles of dependability, trustworthiness and resilience. Securing the design through the application of best practice principles is recommended, including defence in depth and threat modelling. A thorough functionality and security verification of the model must be performed.

- **Security verification and validation testing** – All security requirements for the product must be shown to have been met, and the product's defence in depth strategy shown to be effective when the product is deployed. A requirements based testing approach is required to show that functional and security requirements have been correctly implemented.

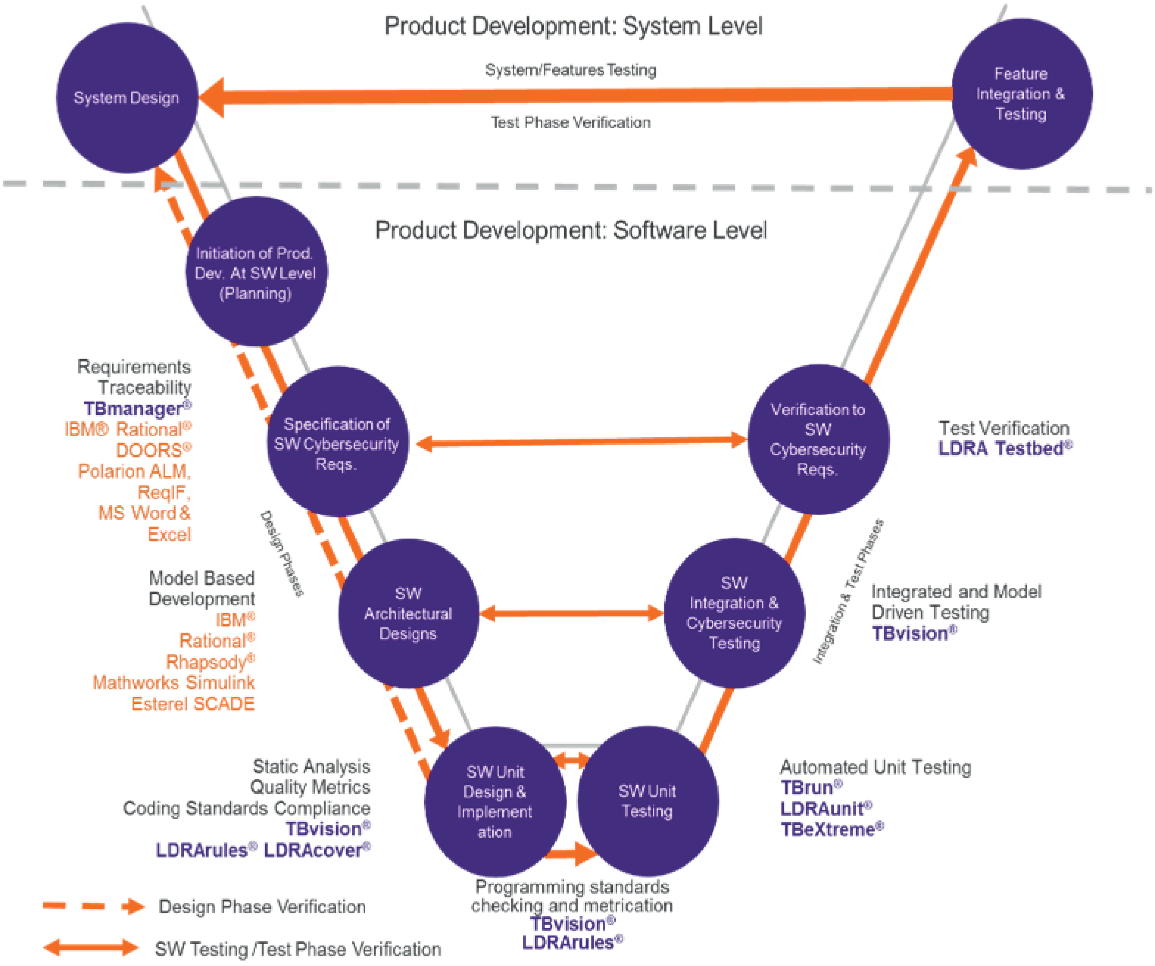
Vulnerability tests are needed to provide assurance that there are no known vulnerabilities in the code. Coding standards like CERT C/C++, CWE, and MISRA help by avoiding such issues at an early stage in the lifecycle.

Security testing can also include additional verification activities including performance, scalability, and robustness tests. Similar in nature to fuzz testing for web applications, robustness tests are designed to show that correct functionality is retained in the face of a range of inputs, often derived from boundary value analysis, error guessing, or error seeding techniques.

Structural coverage analysis helps to identify the uncovered portion of code and thus minimize the possibilities of attack surface in the code.

Structural coverage analysis helps to identify the uncovered portion of code and thus minimize the possibilities of attack surface in the code.

Applying security techniques during the development lifecycle


Product Development: System Level
System Design
System/Features Testing
Test Phase Verification
Feature Integration & Testing
Product Development: Software Level
Initiation of Prod. Dev. At SW Level (Planning)
Requirements Traceability
TBmanager®
IBM® Rational®
DOORS®
Polarion ALM,
ReqIF,
MS Word &
Excel
Specification of SW Cybersecurity Reqs.
Verification to SW Cybersecurity Reqs.
Test Verification
LDRA Testbed®
Design Phases
Model Based Development
IBM®
Rational®
Rhapsody®
Mathworks Simulink
Esterel SCADE
SW Architectural Designs
SW Integration & Cybersecurity Testing
Integration & Test Phases
Integrated and Model Driven Testing
TBvision®
Static Analysis
Quality Metrics
Coding Standards Compliance
TBvision®
LDRArules® LDRAcover®
SW Unit Design & Implement ation
SW Unit Testing
Automated Unit Testing
TBrun®
LDRAunit®
TBeXtreme®
Programming standards checking and metrication
TBvision®
LDRArules®
Design Phase Verification
SW Testing /Test Phase Verification

The challenges inherent in complying with IEC 62443-4-1:2018 guidance can be eased through the use of automated and integrated tools. Verification and validation plays an important role in the process, and several testing techniques are required if the standard's recommendation for requirement based testing is to be complied with.

The LDRA tool suite's static analysis capability contributes to vulnerability analysis by comparing the code with coding standards rules and reporting any violations, and by ensuring that code is developed in accordance with the desired quality level.

Dynamic analysis can be deployed both to verify correct functionality and to further demonstrate security through robustness testing. Code coverage analysis provides assurance that In addition to it, 100% code coverage gives the confidence that the attack surface is minimal.

In summary

- IEC 62443-4-1:2018 ensures the security of electrical/electronic/programmable electronic devices deployed in industrial automation control systems
- It ensures that security measures are built into the product
- Using tools with a proven track record and pedigree to automate the software development process:
  - Provides assurance in the development of a safe and secure product
  - Gives confidence to other stakeholders
  - Saves time and money

LDRA Technology Inc.
2540 King Arthur Blvd, Suite 228
Lewisville, Texas 75056
United States
Tel: +1 (855) 855 5372
e-mail: info@ldra.com

LDRA Technology Pvt. Ltd.
Unit No B-3, 3rd floor Tower B,
Golden Enclave. HAL Airport Road
Bengaluru
560017
India
Tel: +91 80 4080 8707
e-mail: india@ldra.com

www.ldra.com
LDRA

LDRA UK & Worldwide
Portside, Monks Ferry,
Wirral, CH41 5LH
Tel: +44 (0)151 649 9300
e-mail: info@ldra.com

bsi. ISO 9001 Quality Management

SGS TÜV SAAR FUNKTIONALE SICHERHEIT GEPRÜFT FUNCTIONAL SAFETY APPROVED

TÜV SÜD