

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

The IEC 62443 series 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 (Figure 1). 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.

KEY 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

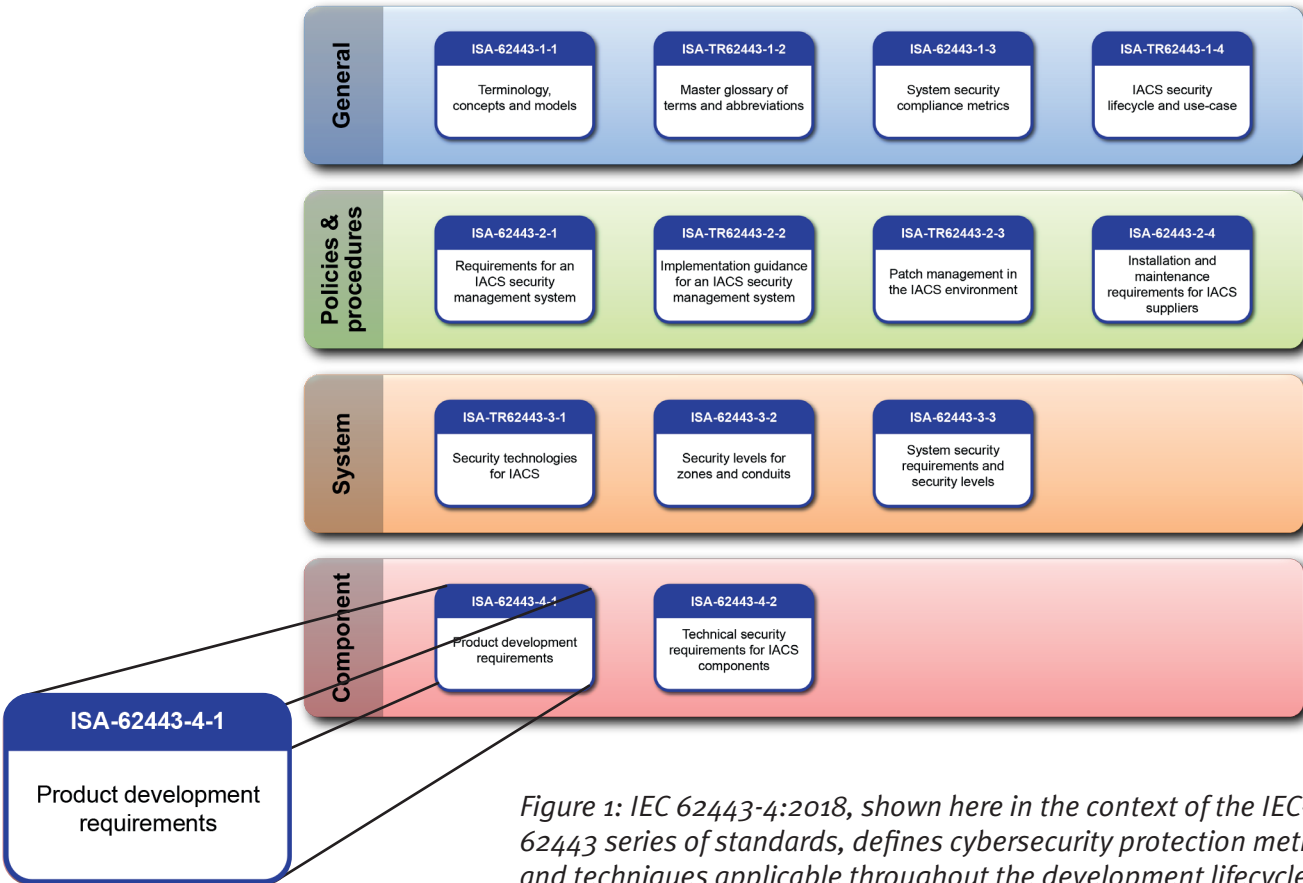


Figure 1: IEC 62443-4:2018, shown here in the context of the IEC-62443 series of standards, defines cybersecurity protection methods and techniques applicable throughout the development lifecycle.

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.

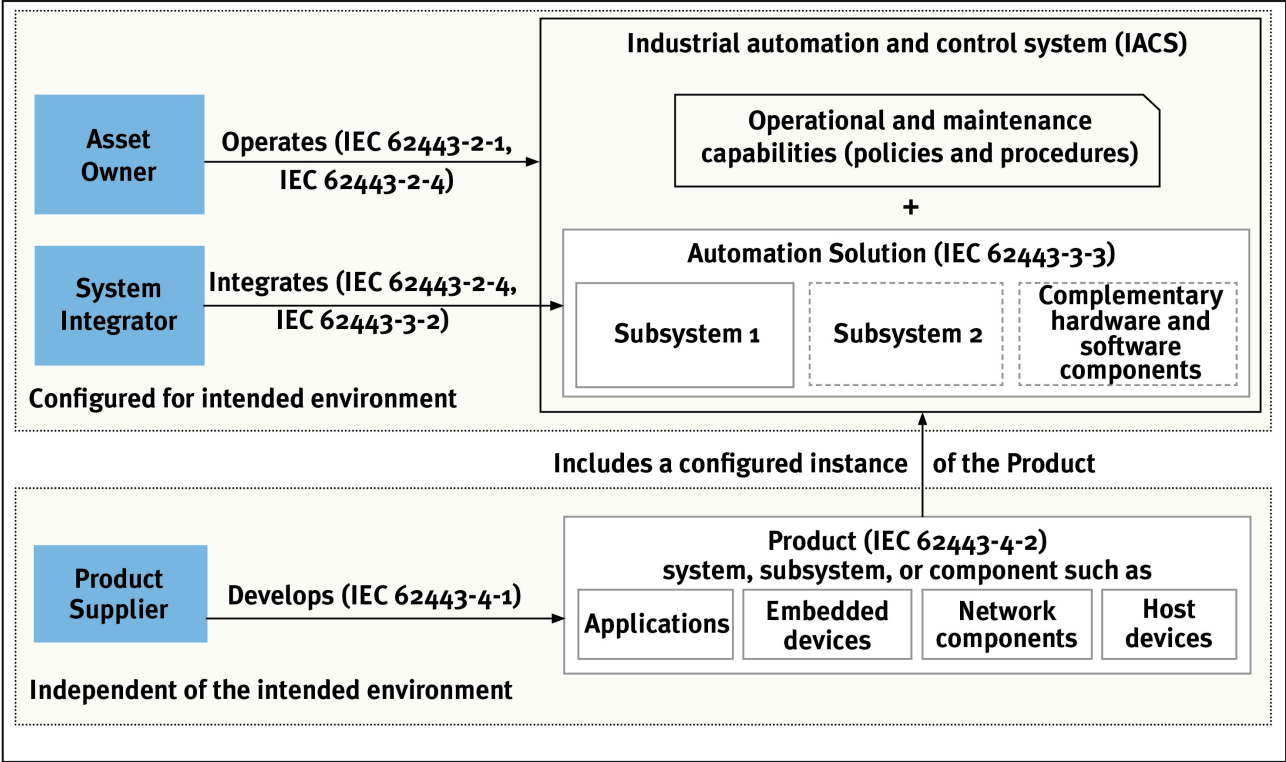


Figure 2: Illustrating the relationships between IACS subsystems

Core objectives of the standard include

- **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 important 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/CPP, 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.

Applying security techniques during the development lifecycle

Traditional practice for secure code verification is largely reactive, meaning that code is developed in accordance with relatively loose guidelines and then tested by means of performance, penetration, load, and functional testing to identify vulnerabilities prior to their being addressed (Figure 3).

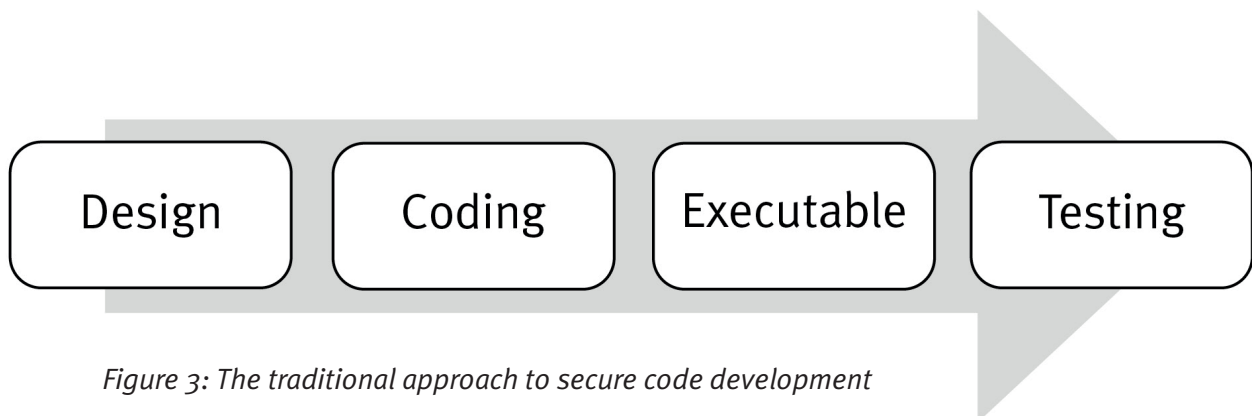


Figure 3: The traditional approach to secure code development

A better, proactive approach is to ensure that code is secure by design. That implies a systematic development process, where the code is written in accordance with secure coding standards, is traceable to security requirements, and is tested to demonstrate compliance with those requirements as development progresses (Figure 4).

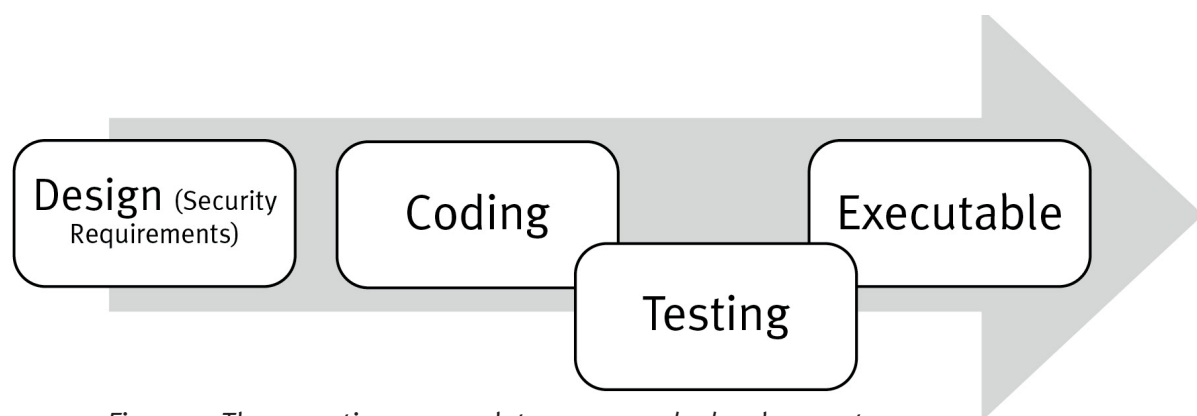


Figure 4: The proactive approach to secure code development

This proactive approach integrates security related best practices into the traditional Software Development Life Cycle (SDLC) that will be familiar to developers in the functional safety domain. The resulting Secure Software Development Life Cycle (SSDLC) represents a “shift left” for application developers, and is a practical approach to ensuring that vulnerabilities are designed out of the system or addressed in a timely and thorough manner.

Figure 5 illustrates how the SSDLC is interpreted by IEC 62443-4-1:2018, and it shows how the challenges inherent in complying with its 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.

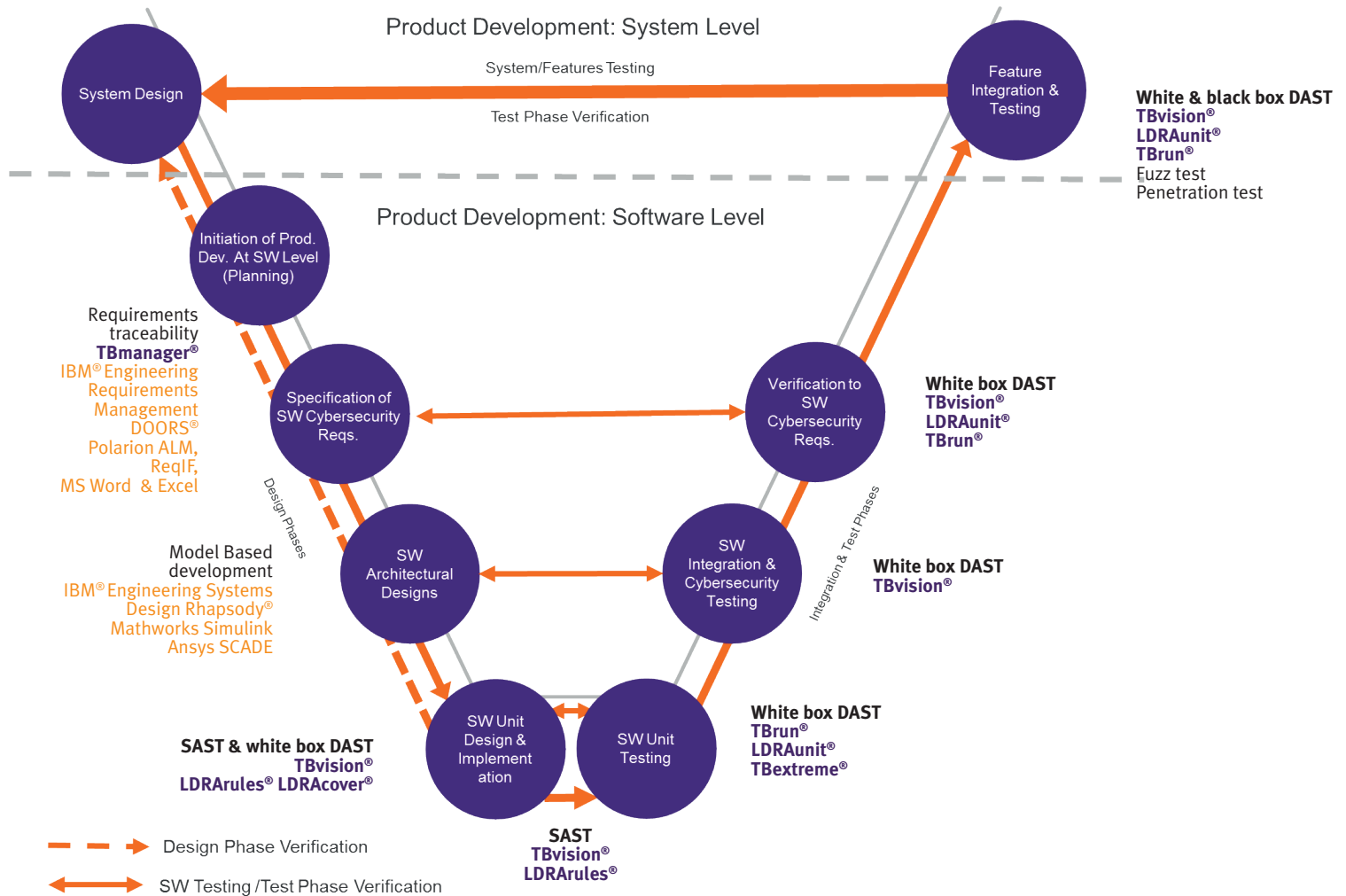


Figure 5: Illustrating the relationships between IACS subsystems

It is an approach that has been proven to work for many years in the functional safety sectors, and which lends itself to appropriate adaptation for the different demands of secure application software. As a consequence, the proven tooling leveraged by SAST, white box DAST, and requirements traceability provide a sound foundation for the cohesive and integrated approach to application security.

The LDRA tool suite’s requirements traceability capabilities are designed to ensure that all security and functional requirements are met. When used in conjunction with white box DAST code coverage, it can also demonstrate that there is no superfluous code in accordance with the objectives of IEC 62443-4-1.

The tool suite’s static analysis (SAST) 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.

In addition to its role in demonstrating the absence of rogue code, the tool suite’s unit and system testing dynamic analysis capabilities (white box DAST) can be deployed to verify correct functionality. They can further demonstrate security through robustness testing which is 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.

Conclusions

Adherence to IEC 62443-4-1:2018 helps to enhance the security of electrical/electronic/programmable electronic devices deployed in industrial automation control systems. It encourages a “shift left” approach to ensuring that security measures are built into the product.

Using tools with a proven track record and pedigree to automate adherence to its recommended software development process including SAST, DAST and requirements traceability provides assurance in the development of a safe and secure product, gives confidence to all stakeholders, and improves efficiency to save time and money.



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

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