INTRODUCTION

There is no simple recipe for how to secure an industrial automation and control system (IACS) and there is good reason for this. It is because security is a matter of risk management. Every IACS presents a different risk to the organization depending upon the threats it is exposed to, the likelihood of those threats arising, the inherent vulnerabilities in the system and the consequences if the system were to be compromised. Furthermore, every organization that owns and operates an IACS has a different tolerance for risk.

This document strives to define a set of engineering measures that will guide an organization through the process of assessing the risk of a particular IACS and identifying and applying security countermeasures to reduce that risk to tolerable levels.

A key concept in this document is the application of IACS security zones and conduits. Zones and conduits are introduced in ISA-62443-1-1. Readers are encouraged to familiarize themselves with these concepts prior to reading this document.

Figure 1 illustrates the relationship of the different parts of ISA-62443 that were in existence or planned as of the date of circulation of this document. Those that are normatively referenced are included as normative references and those that are referenced for informational purposes or that are in development are listed in the Bibliography.

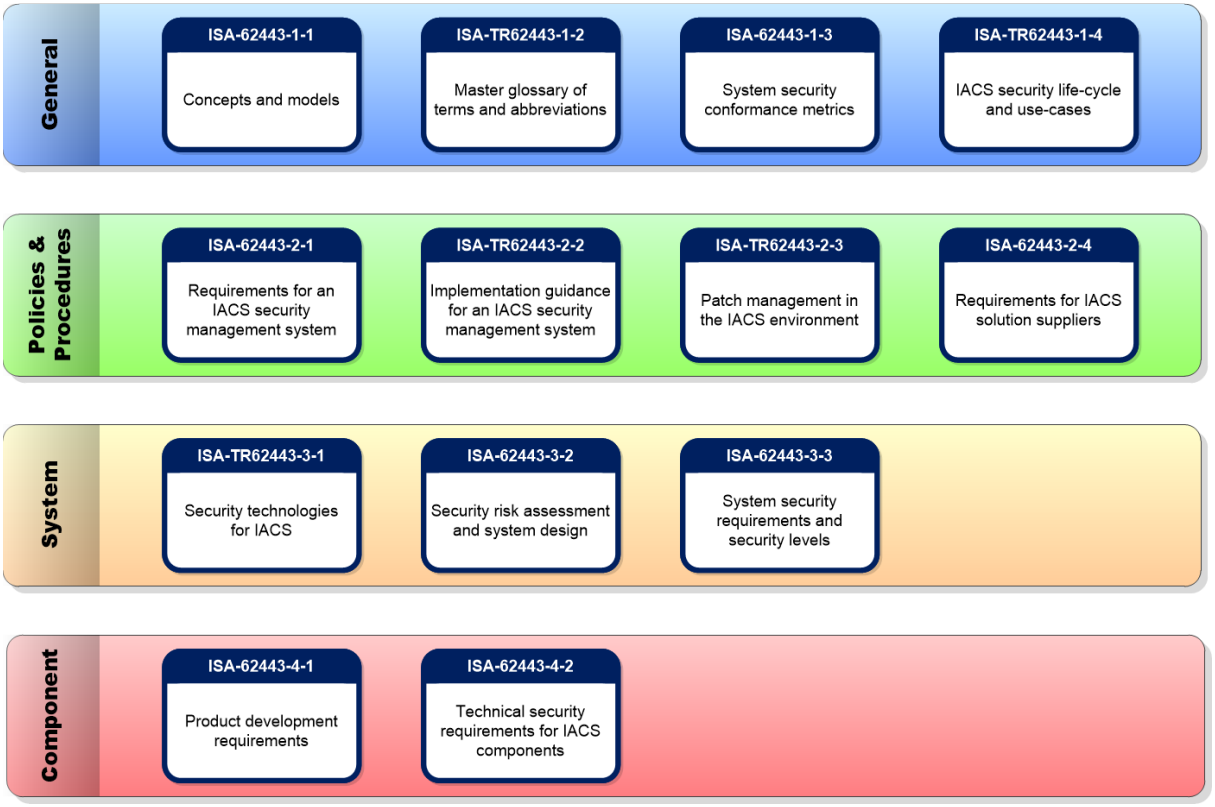

Figure 1 – Parts of the ISA-62443 series

Purpose and intended audience

The audience for this document is intended to include the asset owner, system integrator, product supplier, service provider, and compliance authority.

Usage within other parts of the ISA-62443 series

This document provides a basis for specifying security countermeasures by aligning the target security levels (SL-Ts) identified in this standard with the required capability security levels (SL-Cs) specified in ISA-62443-3-3.

1 Scope

This document establishes requirements for:

- defining a system under consideration (SUC) for an industrial automation and control system (IACS);
- partitioning the SUC into zones and conduits;
- assessing risk for each zone and conduit;
- establishing the target security level (SL-T) for each zone and conduit; and
- documenting the security requirements.

2 Normative references

ISA-62443-1-1, *Security for industrial automation and control systems Part 1-1: Terminology, concepts, and models*

ISA-62443-2-1, *Security for industrial automation and control systems Part 2-1: Establishing an industrial automation and control systems security program*

ISA-62443-3-3, *Security for industrial automation and control systems Part 3-3: System security requirements and security levels*

3 Terms, definitions, abbreviated terms, acronyms and conventions

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions given in ISA-62443-1-2 [1][1] and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at http://www.electropedia.org/

3.1.1
channel
specific logical or physical communication link between assets

Note 1 to entry: A channel facilitates the establishment of a connection.

3.1.2
compliance authority
entity with jurisdiction to determine the adequacy of a security assessment or the effectiveness of implementation as specified in a governing document

Note 1 to entry: Examples of compliance authorities include government agencies, regulators, external and internal auditors.

3.1.3
conduit
logical grouping of communication channels that share common security requirements connecting two or more zones

[1] Numbers in brackets indicate references in the Bibliography.