# SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

# Part 3-2: Security risk assessment for system design



## 1 Scope

This part of IEC 62443 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

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62443-3-3:2013, *Industrial communication networks – Network and system security – 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 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.