Security

Go up to Terms and Definitions

Discussion

Security is a Quality Characteristic concerning the degree to which a subject protects information, operations, and resources so Actors and systems receive access appropriate to their authorization.

Security can apply to:

- A Candidate Solution
- A Distributed System
- A Node
- A Node Set
- A service
- A software component
- A hardware component
- An Endpoint
- An Execution Facility
- An Operational Resource
- A Test Environment
- Information
- Another subject requiring protection

Security can concern:

- Confidentiality
- Integrity
- Availability
- Authenticity
- Accountability
- Non-repudiation
- Authorization
- Access control
- Isolation
- Protection of communications
- Protection of stored information
- Protection of credentials
- Protection of Evidence
- Detection of security events
- Response to security events
- Another security property

Security can identify:

- The evaluated subject
- The protected information

- The protected operations
- The protected resources
- The applicable Actors
- The applicable Roles
- The applicable Authorities
- The applicable authorization rules
- The applicable threats
- The applicable vulnerabilities
- The applicable security controls
- The applicable security events
- The applicable Governance Policies
- The applicable Validation Criteria
- The applicable Acceptance Criteria
- Its Evidence
- Its Provenance
- Its Traceability

Security can be evaluated by determining whether the subject:

- Permits authorized operations
- Refuses unauthorized operations
- Protects information in transit
- Protects information at rest
- Protects information during processing
- Preserves information integrity
- Preserves operation integrity
- Authenticates applicable Actors and systems
- Records security-relevant events
- Detects applicable security conditions
- Responds according to applicable Governance Policies
- Maintains required isolation boundaries
- Preserves required Evidence

Definition

Quality Characteristic concerning the degree to which a subject protects information, operations, and resources so Actors and systems receive access appropriate to their authorization

Source

Adapted from:

- ISO/IEC 25010:2023, Systems and software Quality Requirements and Evaluation (SQuaRE) — Product quality model
- Quality Characteristic
- Governance Policy

- DIDO Reference Implementation Conceptual Model
- DIDO-TE draft Requirements Register

ISO/IEC 25010 identifies Security as a product-quality characteristic concerning protection of information and data according to applicable authorization.

This definition extends the evaluated subject to include DIDO-TE operations, resources, Test Environments, Nodes, Node Sets, Evidence, and other protected subjects.

Note

Security is a broad Quality Characteristic. A requirement should identify the specific security property, subject, threat, condition, and required outcome.

A statement that a subject **shall be secure** does not establish an objectively verifiable obligation.

Security differs from safety:

- Security concerns protection against unauthorized access, use, disclosure, alteration, disruption, or control
- Safety concerns protection from unacceptable risk of physical injury, damage, or harm

Security differs from Reliability:

- Security concerns protection according to authorization and security constraints
- Reliability concerns sustained performance of specified functions under specified conditions

A security event can affect Reliability, but Security and Reliability remain separate Quality Characteristics.

Security differs from Compliance:

- Security identifies a quality property
- Compliance concerns satisfaction of applicable Requirements, policies, standards, laws, regulations, or controls

A subject can implement strong security controls while failing to comply with a particular security requirement.

A subject can comply with specified minimum controls while retaining security risks not addressed by those controls.

Security evaluation should identify:

- The applicable security context
- The applicable threat assumptions
- The applicable authorization model
- The protected subjects
- The applicable security controls
- The evaluation methods
- The permitted residual risk

- The required Evidence

Example

DIDO-TE evaluates three Candidate Solutions that provide the same Node function.

The Acceptance Criteria establish security evaluations for:

- Actor authentication
- Operation authorization
- Communication confidentiality
- Communication integrity
- Stored-information protection
- Tenant isolation
- Security-event recording
- Evidence preservation

DIDO-TE performs the applicable Test Definitions and records the Test Results, Verdicts, security events, and supporting Evidence for each Candidate Solution.

The comparative evaluation identifies differences among the Candidate Solutions without treating Security as one undefined aggregate score.
