CPS Security Standards/Guidelines

S. Venkatesan

IIIT Allahabad

Acknowledgement: The contents, example scripts and some figures are copied from various sources.
Thanks to all authors and sources made those contents public and usable for educational purpose

Introduction

- U.S. National Science Foundation
  - *A system that "integrate[s] sensing, computation, control and networking into physical objects and infrastructure, connecting them to the Internet and to each other.*

- The term "cyber-physical systems" was coined by Helen Gill at the National Science Foundation in the United States.

- The key element in the implementation of the concepts of Industry 4.0 is the idea of **cyber-physical systems (CPS)**.

- CPS is an integration of computational and communication capabilities with physical processes and assets,
  - such as buildings, vehicles, equipment, instruments, sensors, and actuators, to monitor, control, automate, and optimize these processes and assets,
  - leading to improved safety, performance and efficiency.

NIST Cyber Security Framework

- Govern
- Identify
- Protect
- Detect
- Respond
- Recover

Foundational Requirements: IEC62443

- **IEC62443 series d**efine requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS).

- Foundational Requirements
  - FR 1 – Identification and authentication control (IAC)
  - FR 2 – Use control (UC)
  - FR 3 – System integrity (SI)
  - FR 4 – Data confidentiality (DC)
  - FR 5 – Restricted data flow (RDF)
  - FR 6 – Timely response to events (TRE)
  - FR 7 – Resource availability (RA)

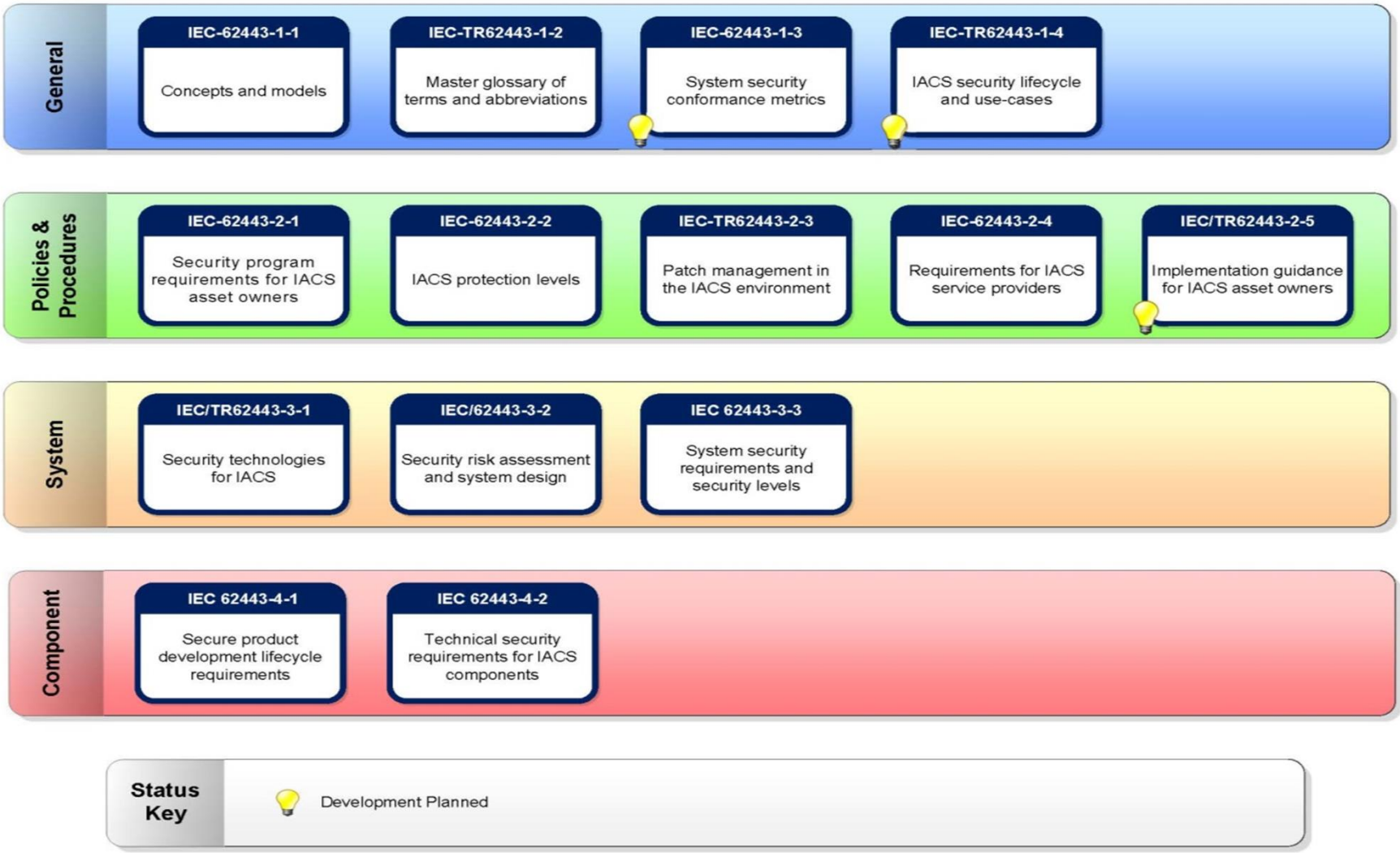
Design Principles: **IEC62443**

- Secure by Design
- Reduce Attack Surface
  - Access Control
  - Network segmentation
  - Least function
  - Least privilege
- Defense in Depth [Layers of Protection]
- Essential Functions to avoid loss of control, view, protection
  - the safety instrumented function (SIF)
  - the control function
  - the ability of the operator to view and manipulate the EUC(Equipment Under Control)

Principal Roles: IEC62443

- Asset Owner: Accountable and responsible for the IACS also the operator of the IACS and the EUC.
- Maintenance Service Provider: provides support activities for an automation solution.
- Integration Service Provider: provides integration activities for an automation solution including design, installation, configuration, testing, commissioning and handover to the asset owner.
- Product Supplier: that manufactures and supports a hardware and/or software products.

IEC 62443 Series of Industrial Security Standard – Overview (ISA99.org)



https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62443/

IEC 62351

- For Energy Management System focuses on
  - confidentiality,
  - data integrity,
  - authentication
  - non-repudiation.

- IEC 61850 - two main factors: ease of connection via Ethernet instead of the traditional hardwired systems and standardized message structures that ensure interoperability.
  - Security issues of this is handled by IEC62351

- Goose (Generic Object Oriented Substation Event) and SV (Sample Value) message – SHA and RSA for Digital Signature

IEC 62351 - Parts

- Part 1: Introduction to security issues.
- Part 2: Glossary of terms.
- Part 3: Profiles including TCP/IP.
- Part 4: Profiles including Manufacturing Message Specification (MMS) and derivatives.
- Part 5: Security for IEC 60870-5 and derivatives.
- Part 6: Security for IEC 61850.
- Part 7: Network and system management (NSM) data object models.
- Part 8: Role-based access control.
- Part9: Cyber security key management for power system equipment.
- Part 10: Security architecture guidelines.
- Part 11: Security for eXtensible markup language (XML) documents.
- Part 12: Resilience and security recommendations for power systems with DER cyber-physical systems.
- Part 13: Guidelines on security topics to be covered in standards and specifications.
- Part 90-1: Guidelines for handling role-based access control in power systems.
- Part 90-2: Deep packet inspection of encrypted communications.
- Part 100-1: Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7.

NIST SP 800-82r3

- For establishing secure operational technology (OT) while addressing OT's unique performance, reliability, and safety requirements.

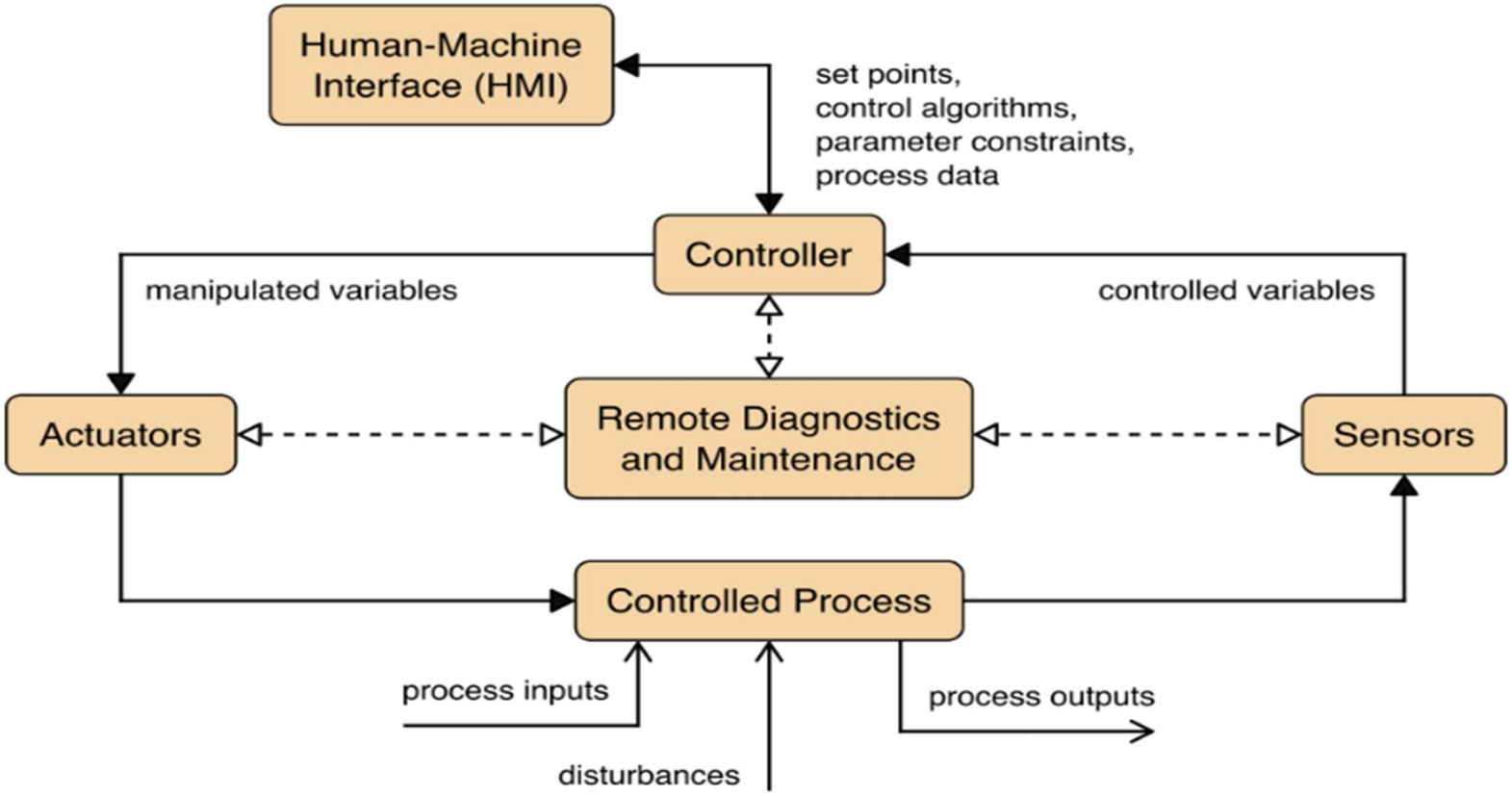


Fig. 1. Basic operation of a typical OT system

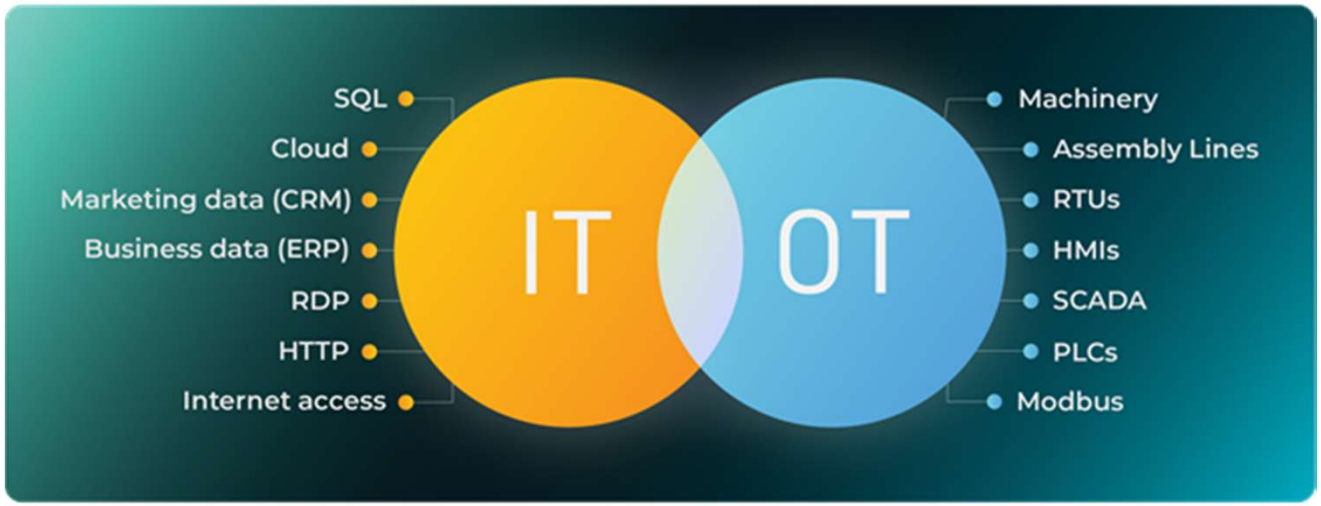
OT System Design Considerations

- Safety
- Control timing requirements
- Geographic distribution
- Hierarchy
- Control Complexity
- Availability
- Impact of Failures

OT and IT System Security

- Timeliness and performance requirements.
- Availability requirements.
- Risk management requirements.
- Physical effects.
- System operation.
- Resource constraints.
- Communications.
- Change management.
- Component Lifetime.
- Component location.

IT vs OT



The hardware and software that monitor and control the physical components of an industrial network are often referred to as Operational Technology (OT).

OT is unique in that it bridges the gap between the physical and digital worlds.

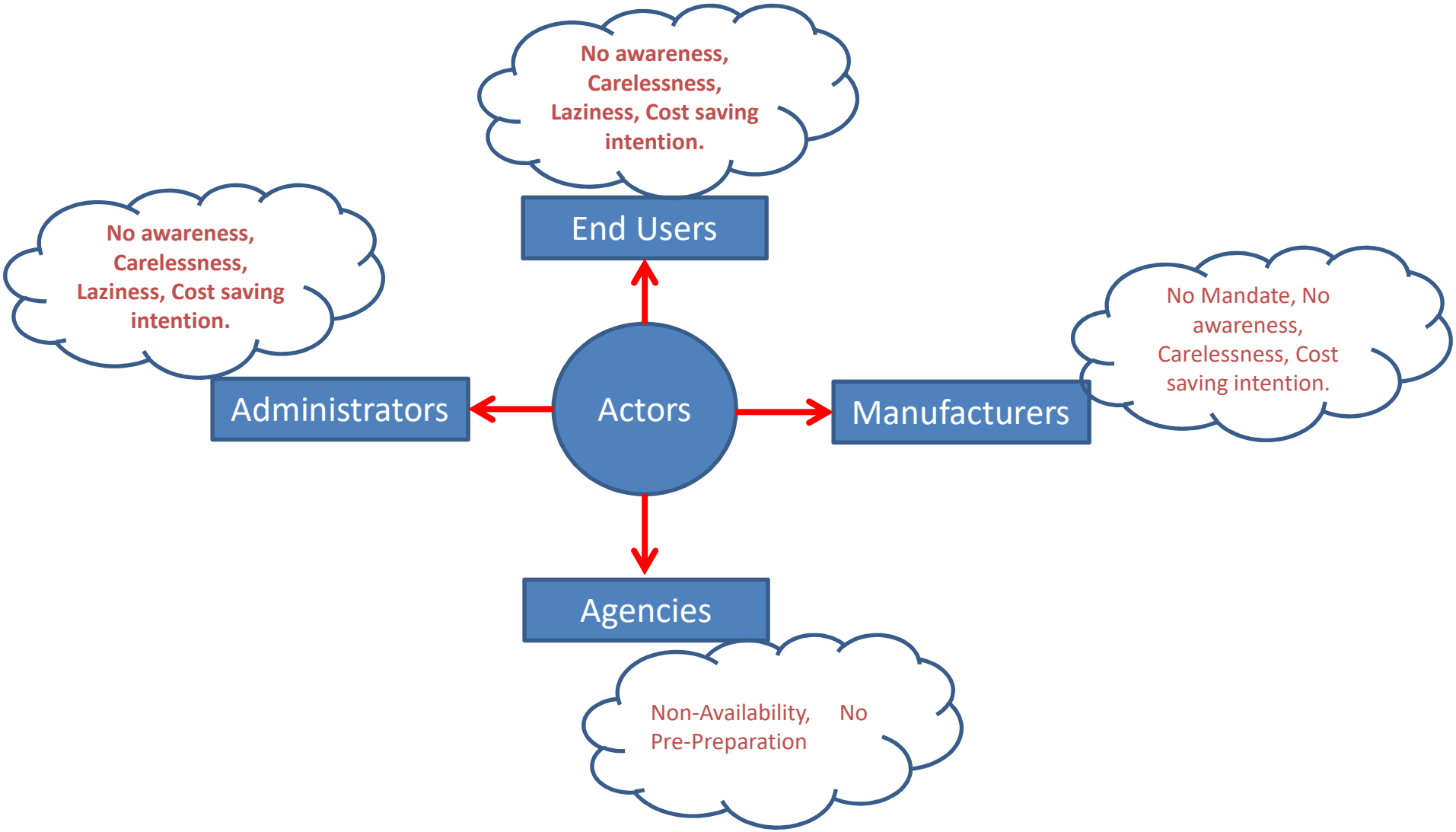
https://www.otorio.com/blog/it-security-vs-ot-security-the-operational-technology-cybersecurity-guide-for-industry-professionals/

OT Security	IT Security
Requirement safety and availability	Confidentiality, Integrity, Availability, so on
Less entry points	More entry points
Complete shutdown for patching	It can be managed
Since OT components are rarely updated, they may have many more public vulnerabilities when compared to IT computers.	
	IT components advance so fast and have relatively short life spans, that a network can look completely different only several years apart.
Magnitude of compromise is high	It is comparatively low
Since patching OT components requires complete shutdowns that halts production, vendors running OT networks rarely patch their components, if at all. This means that the probability of a successful exploit on an OT system is exponentially higher than on an IT system.	Frequent update
OT focuses on the use of digital technology to monitor and control physical processes	IOT/IT security is focused on safeguarding communication between connected devices.

IoT Security Guidelines

- IoT is used in numerous applications such as Home Automation, Manufacturing Industry, Health, and Smart Transportation.
- There are large number of manufacturers for IoT devices.
- Importance is on performance however concentration of the security requirements is minimal.
- The security issues of IoT devices brings data leakage, service disruption, etc.
- End users are not worried about security also have less/no knowledge on Security.

Actors: Responsible for Security Issues



Important Note: Following discussion is in general because there are manufactures/agencies completely or partially fulfilling the requirements

End Users

- Uses the default or weak credentials.
- Devices placed in public places allow attackers to capture the traffic (where users are mandated to place in the public place).
- Non Reporting of known or identified vulnerabilities/attacks.
- Buying IoT devices considering cost, easiness and efficiency not the security aspect.
- Improper configuration of device, fail updating software/firmware.

Administrators

- Uses the default or weak credentials.
- Devices placed in public places allow attackers to capture the traffic (where users are mandated to place in the public place).
- Non Reporting of known or identified vulnerabilities/attacks.
- Buying IoT devices considering cost, easiness and efficiency not the security aspect.
- Improper configuration of device, fail updating software/firmware.
- Not follows security standards.

Manufacturers

- Not providing easy update mechanisms for software/firmware.
- Not having security vulnerability reporting team.
- Not forcing users for strong security such as changing the default password and restrict the weak passwords.
- Not hardening the device configuration.
- Using insecure protocol or algorithm.
- Lack of compliance to security requirements or security standards.
- Non-continuation of business thus no support to the users.
- Neglect security vulnerability reporting.

Agencies

- No standards for the manufacturer and administrators.
- Not providing the awareness to the users.
- No tracking of the manufacturers and products.
- No security vulnerability reporting of the products.

Comparison of Security Guidelines: Missing Security Requirements

Standards or Guidelines	Physical Security	Hardware Security	Software Security	Data Security	Network Security	Management Security	Life Cycle Management	Application Programming Interface (API) Security
1) NIST Security Requirement	A1, A3, A4	D1, D2, D3	E6, E7	B3, B6, B7	C2, C3	F2, F4, F8, F9, F11	G4	H1, H2, H3, H4, H5
2) UK Govern. Requirement	A1, A3, A4	D2, D3	-	B4, B5, B7(P)	C3	F3, F5, F6, F7, F11	G1, G3, G4	H2, H3, H4, H5
3) CIS Critical Security Controls (Version 6): IoT Security	A1, A2, A3, A4	D2, D3	E1, E2, E3, E7	B3, B4, B6, B7	C4	F2, F3, F6, F7, F9, F11	G1, G2, G3	$, H1, H2, H3, H4, H5
4) IoT Security Maturity Model: ISA/IEC 62443	A4	D2, D3, D4	E2, E3, E6	B7(P)	-	F7, F8, F9, F11	-	H1, H2, H3, H4, H5
5) TEC 31318:2021	A1, A3, A4	D2, D3	-	B4, B5, B7(P)	C3	F5, F6, F7, F11	G1, G3, G4	H2, H3, H4, H5
6) IMDA IoT Cyber Security Guide V1	A3, A4	D2, D3, D4	E1, E2, E3, E4, E6, E7	B5, B6, B7	C2, C3, C4	F2, F4, F7, F9, F11	G1, G2, G3	H1, H2, H3, H4, H5
7) IoTSF Secure Design Best Practice	A1, A3	D3	E2, E3, E6	B6, B7	C4	F2, F5, F9, F11	G2, G3, G4	H1, H2, H3, H4, H5
8) DSCI	A1, A3, A4	D2, D3	-	B4, B5, B7(P)	C3	F5, F6, F7, F11	G1, G3, G4	H2, H3, H4, H5
9) ACSC	A1, A3, A4	D2, D3	-	B4, B5, B7(P)	C3	F5, F6, F7, F11	G1, G3, G4	H1, H2, H3, H4, H5
10) ENISA	A3, A4(P)	D1, D3, D4(P)	E2, E3, E7	B3, B6, B7	C2, C3, C4(P)	F2, F3, F4, F5, F6, F11	-	$, H1, H2, H3, H4, H5

For more information, visit https://security.iiita.ac.in/iot/report.php

Comparison of Security Guidelines: Missing Security Requirements

Standards or Guidelines	Physical Security	Hardware Security	Software Security	Data Security	Network Security	Management Security	Life Cycle Management	Application Programming Interface (API) Security
11) Egypt: NTRA	A1	-	E2, E3	**B7**	C3 (P)	F2, F8, F9, F10, F11	G1 (P)	H1, H2, H3, H4, H5
12) Singapore Computer Society	A1,A3, A4(P)	D2, D3, D4(P)	E2, E3, E6, E7(P)	B4, B5, B6, B7	C2(P), C3, C4	F5, F6, F7, F8, F9, F11	G1, G2	H1, H2, H3, H4, H5
13) National Cyber Security Authority, Saudi	A1,A3, A4(P)	D2, D3, D4(P)	E2, E3, E4, E5, E6, E7(P)	B6, B7(P)	C2, C3, C4(P)	F7, F8, **F11**	-	H1, H2, H3, H4, H5
14) IEEE	A1,A2(P), A3, A4	D2, D3, D4(P)	E1, E2, E3, E4, E5, E6, E7	B3, B4, B5, B6, B7	C2, C4(P)	F4, F5, F6, F7, F8, F9, F10, F11	G1, G3	H1, H2, H3, H4, H5
15) Securebydesign	A1, A2, A3, A4	D1, D2, D3, D4	E1, E3, E4, E5, E7	B1, B2, B3, B4, B5, B6, B7	C1, C2, C3, C4	F2, F5, F6, F7, F8, F9, F10, F11	G1, G2, G3, G4	H1, H2, H3, H4, H5
16) IIC	A1(P)	D1, D2, D3, D4	E1(P), E2(P), E3, E4, E7	B1, B2, B3 (P), B6, B7	C1, C2, C3, C4	F1, F2, F3, F4, F6, F7, F8, F9 (P), F10, F11	G2, G3 (P)	H1, H2, H3, H4, H5

*P – Partial

*$– In general discussed the API Security

*API Security is not discussed by majority guidelines/standards because those might have considered it as part of the software security.

References

- https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8918111
- https://en.wikipedia.org/wiki/IEC_62443
- https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62443/
- https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r3.pdf
- https://www.linkedin.com/pulse/cps-cornerstone-industry-40-william-yang
- https://blog.isa.org/cyber-physical-systems-the-core-of-industry-4.0
- https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf