

Series Editor
Jean-Paul Bourrières

Cybersecurity of Industrial Systems

Jean-Marie Flaus

Color section

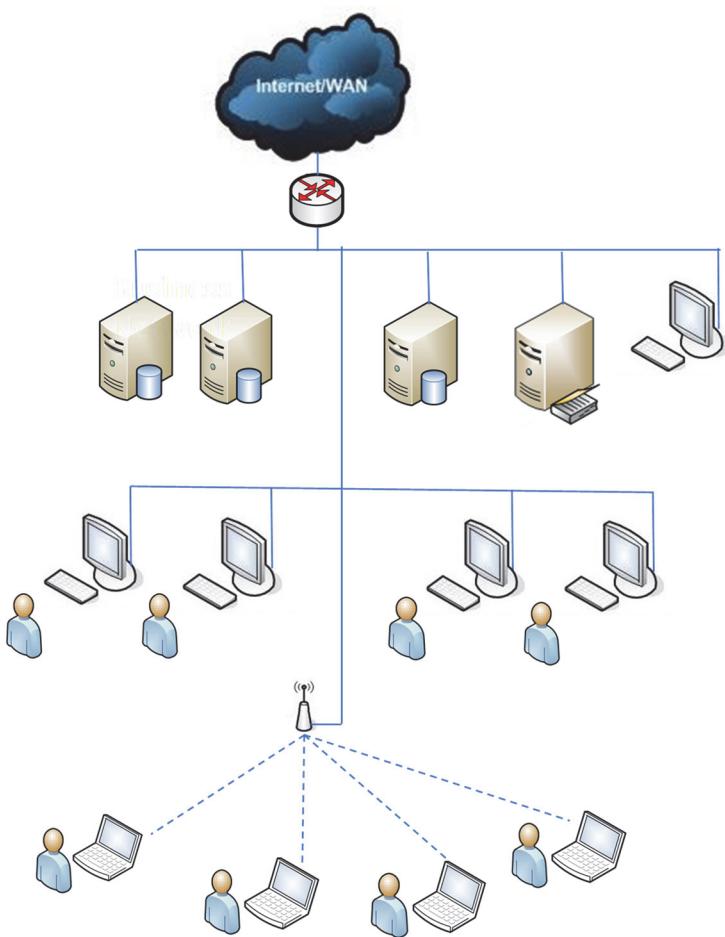


Figure 1.1. Information system

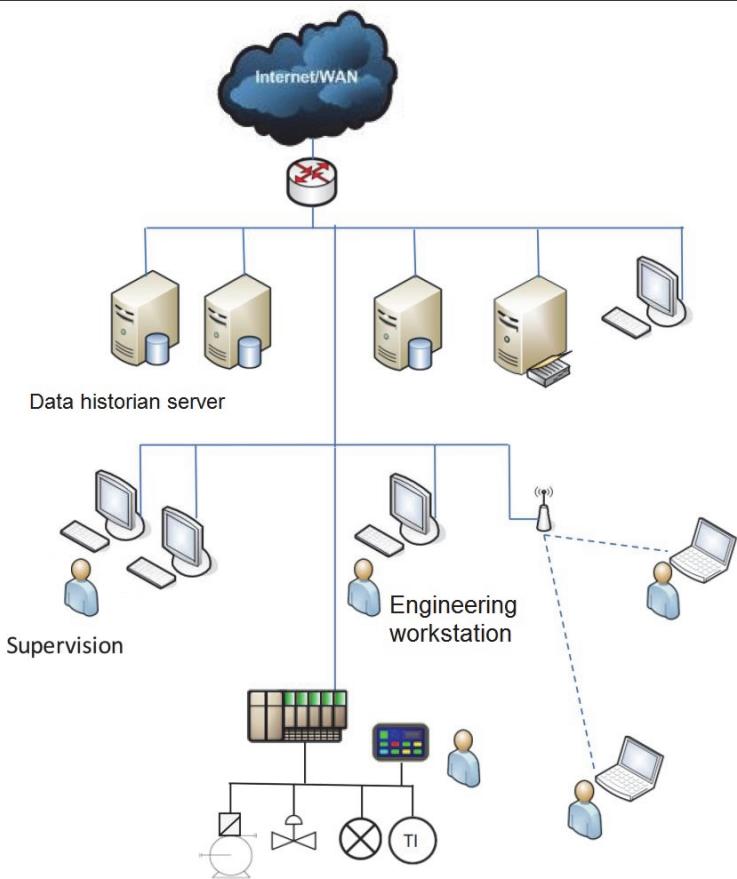


Figure 1.2. Industrial information system

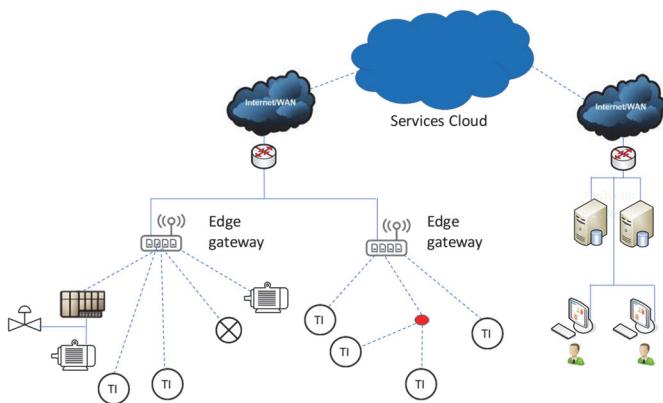


Figure 1.3. IIoT information system

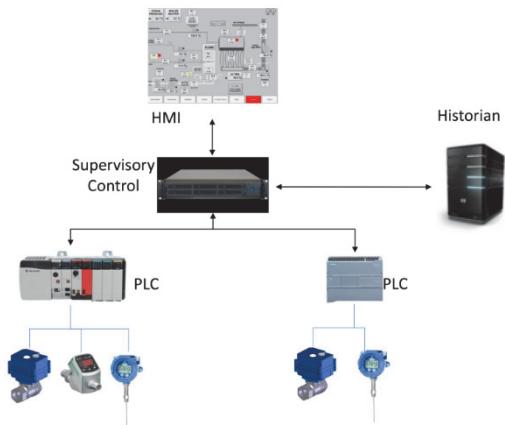


Figure 1.4. The minimal functions of a SCADA

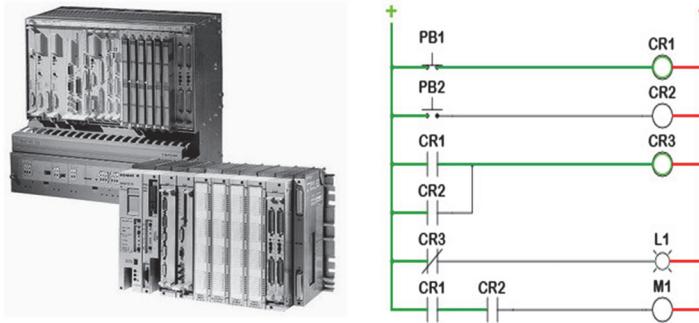


Figure 1.5. Allen Bradley – Modicon 084

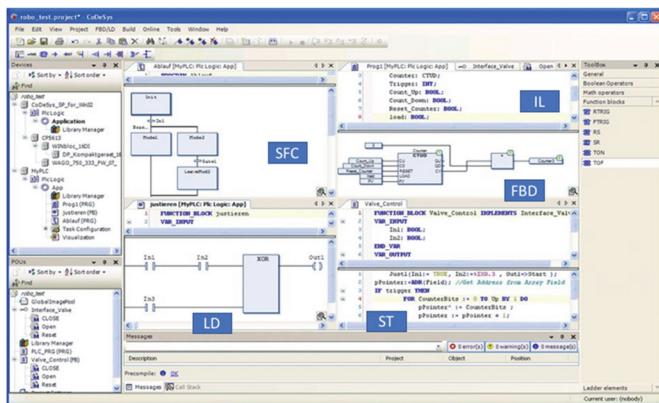


Figure 1.9. Programming languages IEC 61131/3

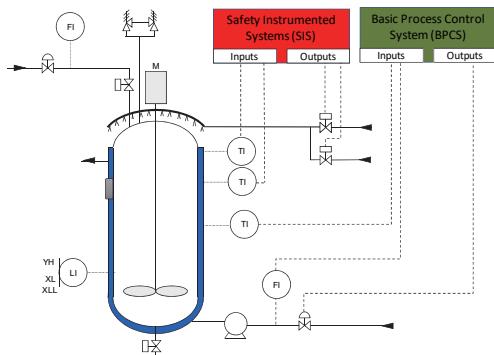


Figure 1.10. Safety instrumented system (SIS)

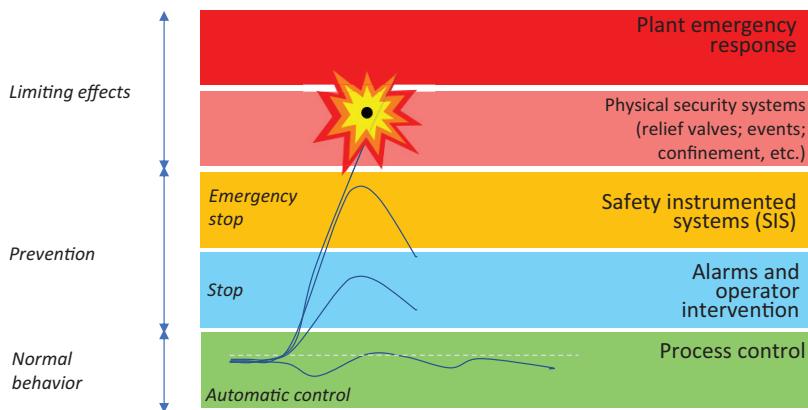


Figure 1.11. The position of the SIS in terms of protection level



Figure 1.12. HMI on PC



Figure 1.13. Dedicated unit for HMI

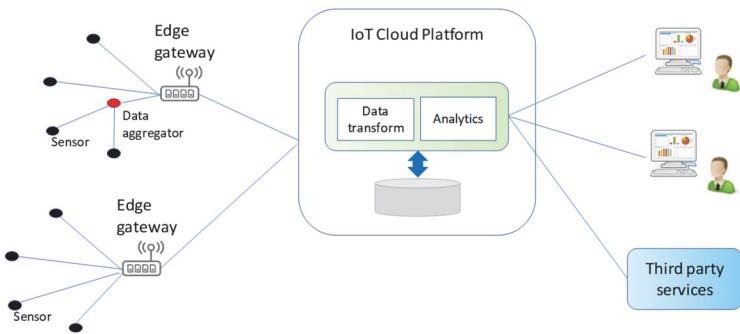


Figure 1.14. IoT platform

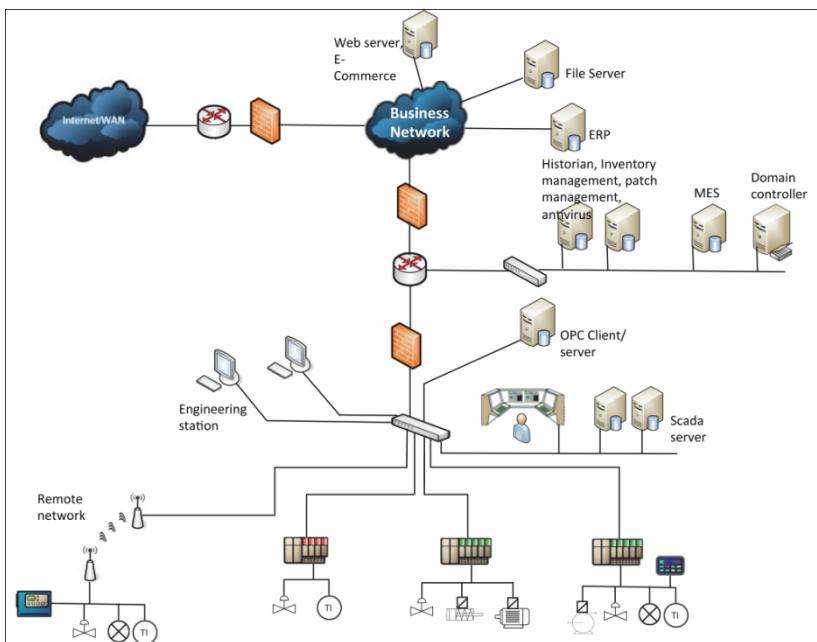


Figure 2.1. Typical ICS architecture

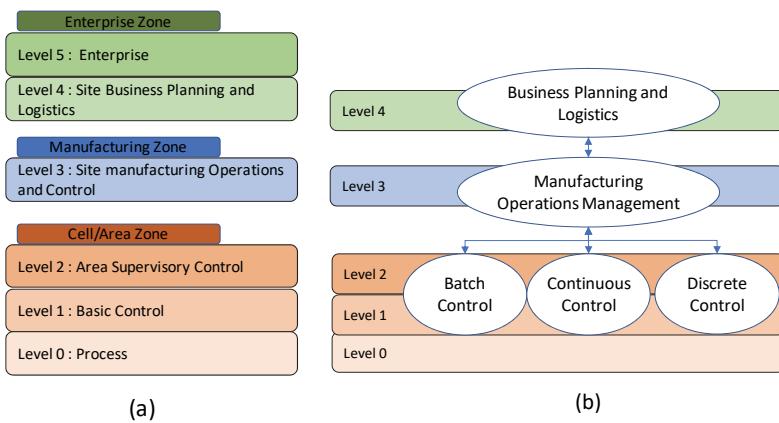


Figure 2.2. (a) *Purdue* and (b) *ISA85* models

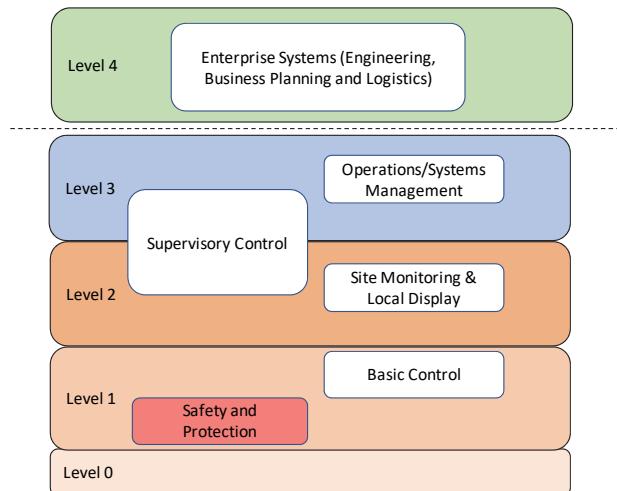


Figure 2.3. IEC 62443 model

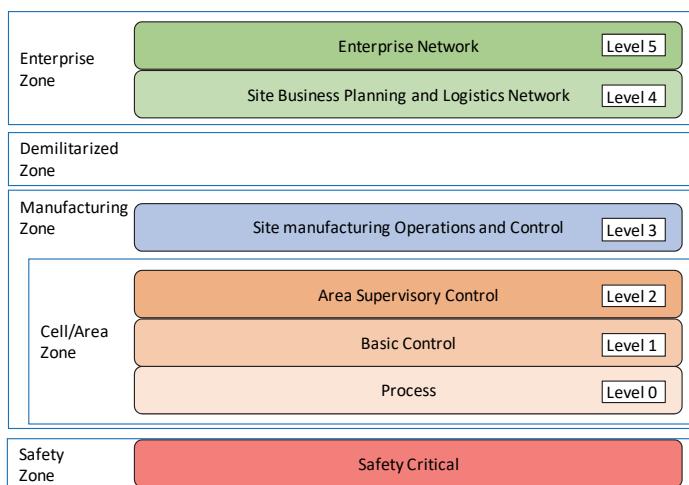


Figure 2.4. Converged Plantwide Ethernet (CPwE) model

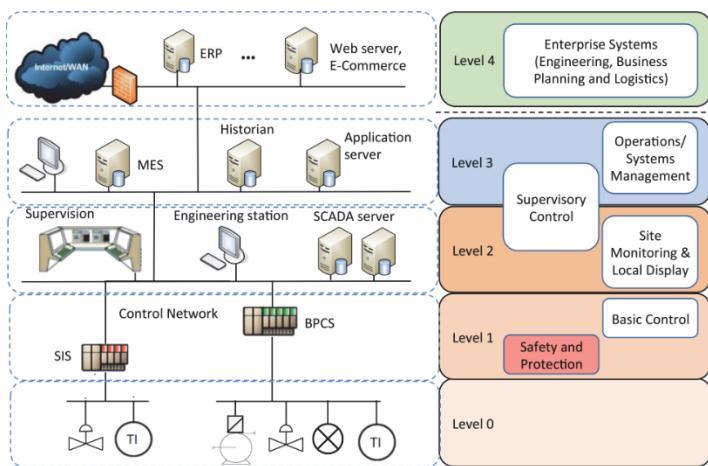


Figure 2.5. Model of the previous installation according to the CIM architecture

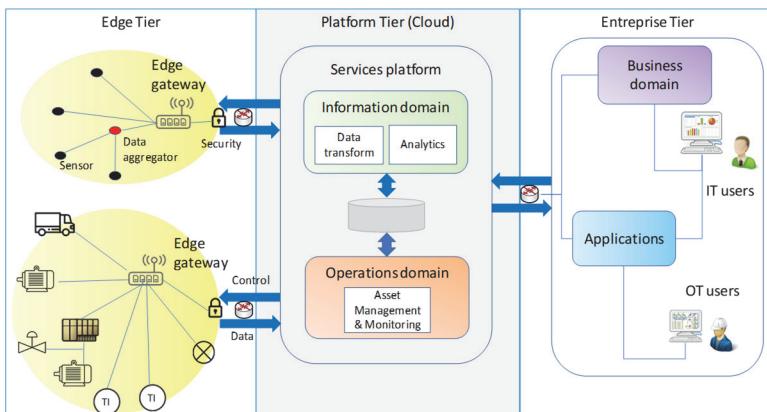


Figure 2.6. IIoT architecture

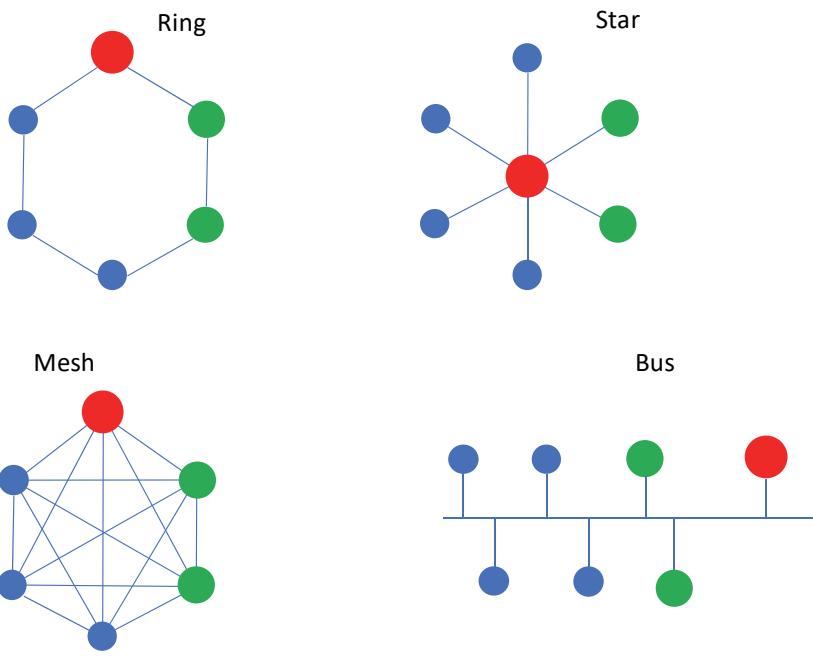


Figure 2.7. Classic network topologies

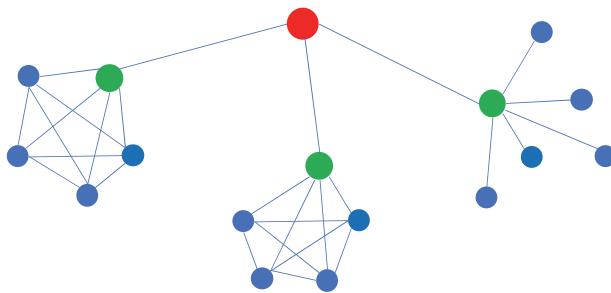


Figure 2.8. Mixed network topology (IIoT)

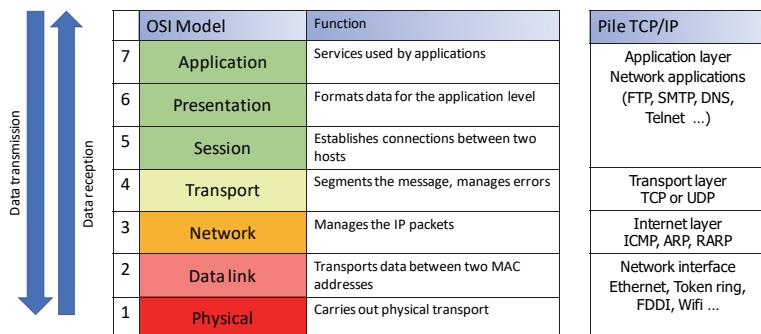


Figure 2.9. OSI models and TCP/IP stack

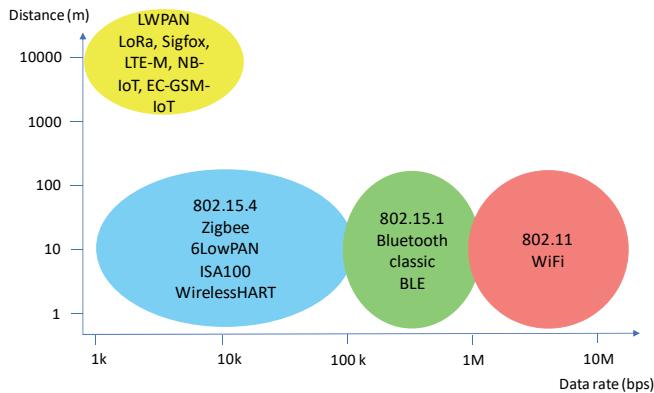


Figure 2.10. Different wireless communication solutions

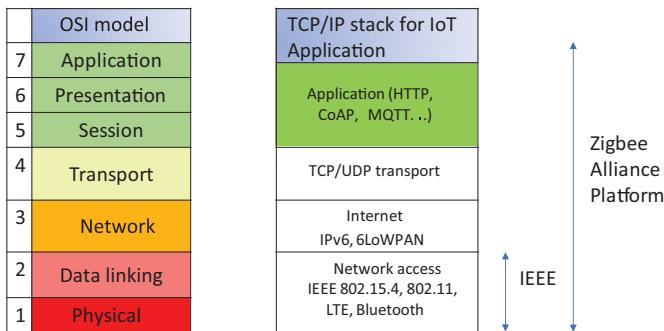


Figure 2.11. IIoT protocols and OSI model

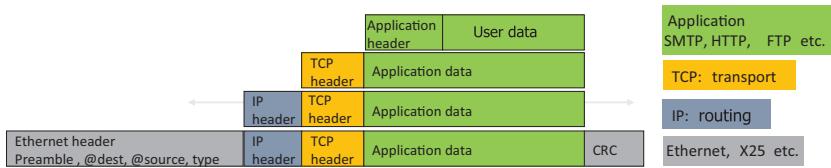


Figure 2.12. Data packages

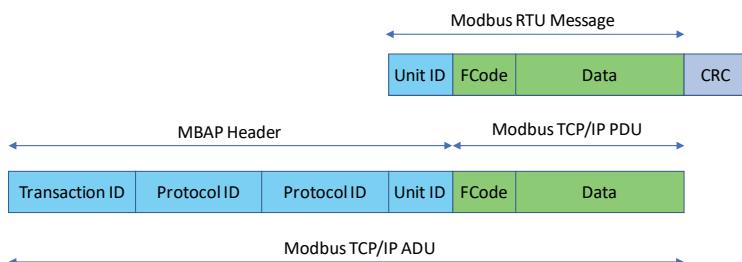


Figure 2.17. Modbus frame

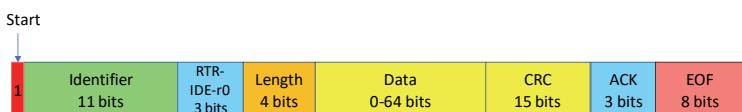


Figure 2.19. CAN frame

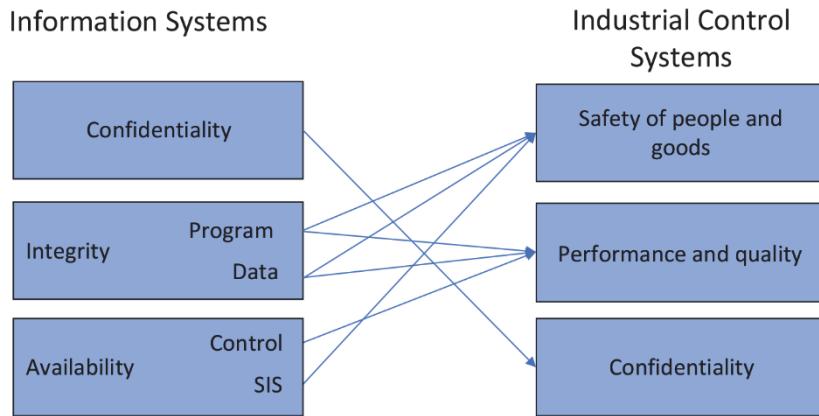


Figure 3.1. Security needs of IS and ICS

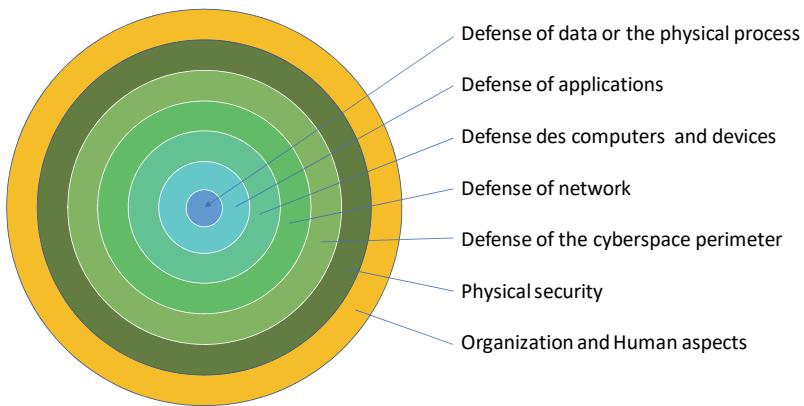


Figure 3.2. The different layers of IT security

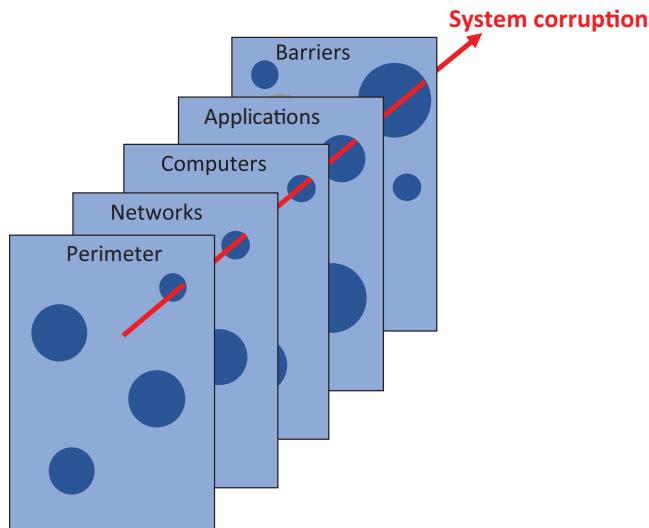


Figure 3.3. Swiss cheese adapted to IT security

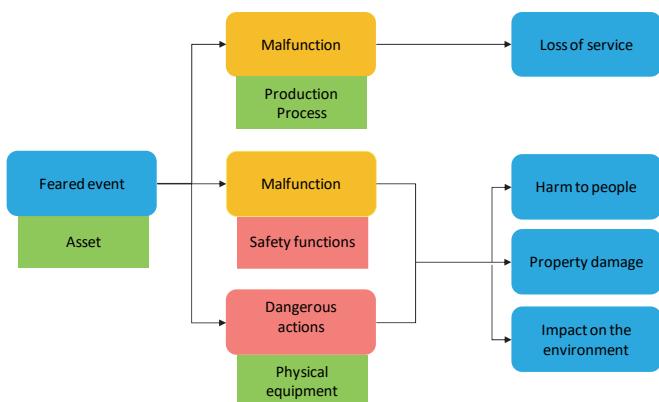


Figure 3.7. Different types of impacts

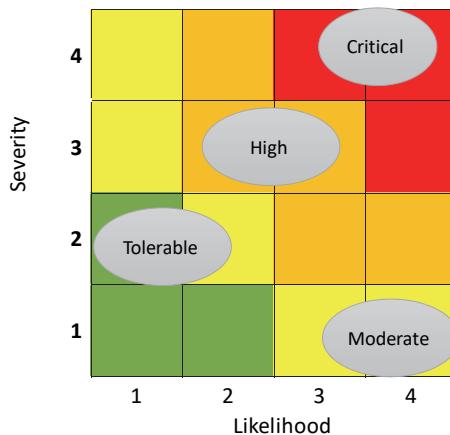


Figure 3.8. Risk matrix or heat map

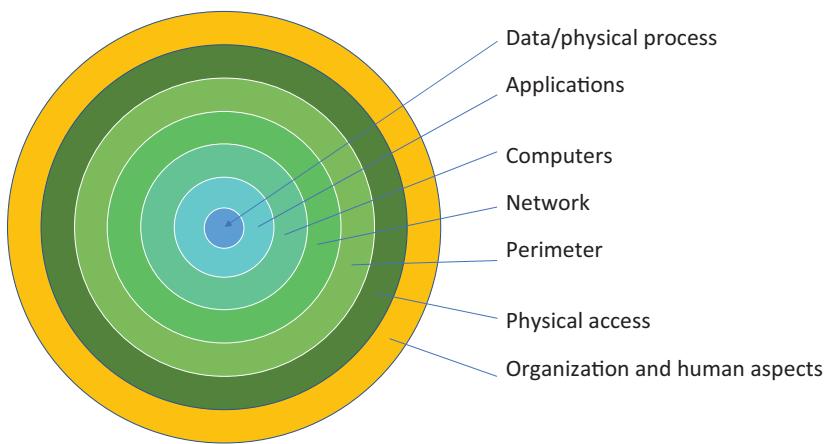


Figure 3.10. Defense in depth

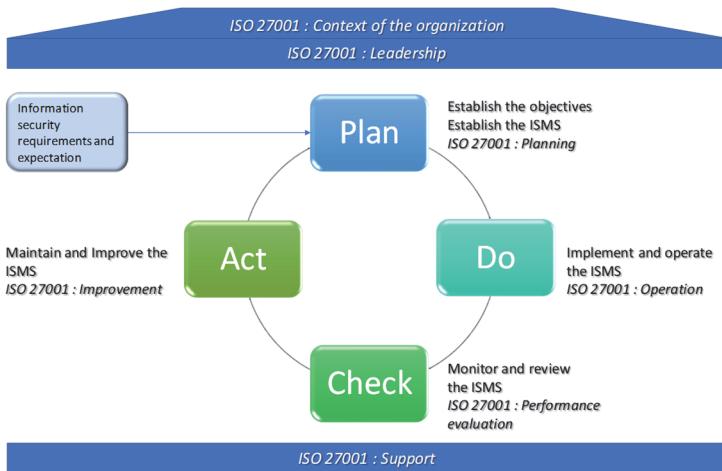


Figure 3.11. Continuous improvement PDCA and ISO 27001:2013

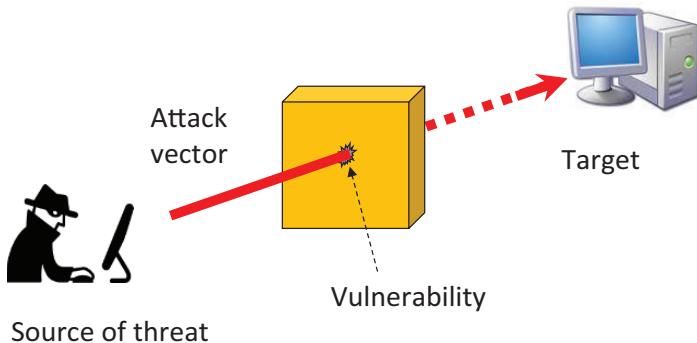


Figure 4.1. Vector of attack and vulnerability

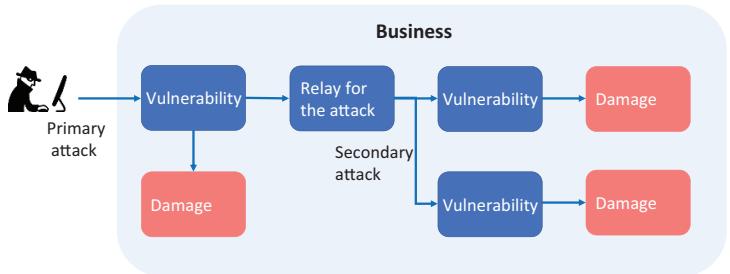


Figure 4.2. Primary and secondary attacks

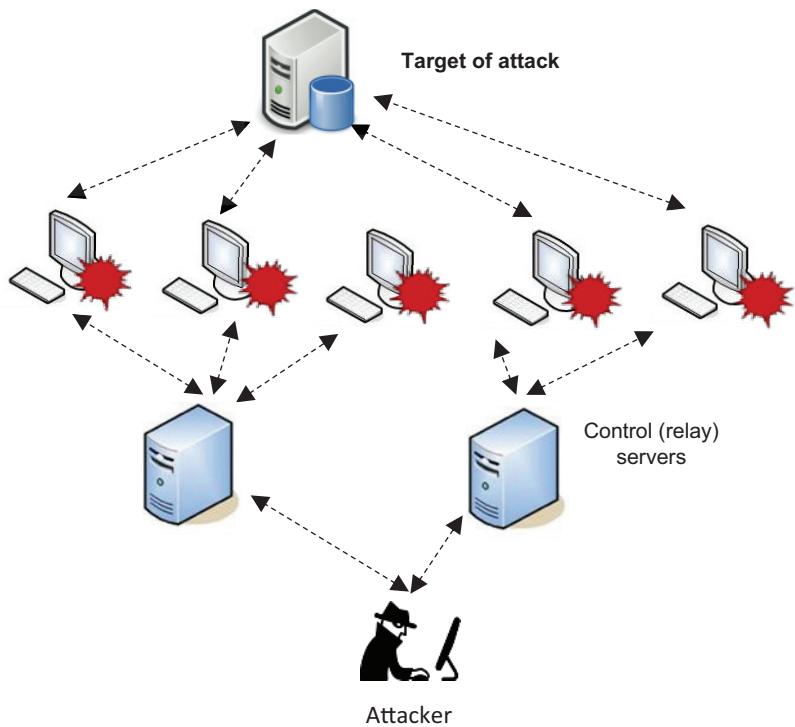


Figure 4.3. DDoS attack by a botnet

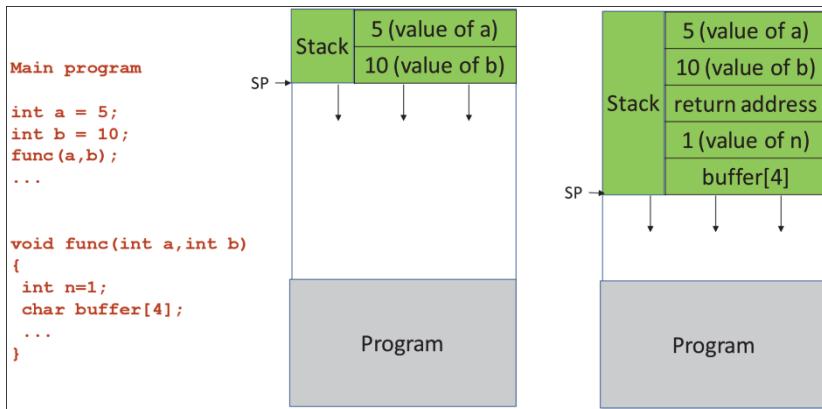


Figure 4.5. Attack by buffer overflow

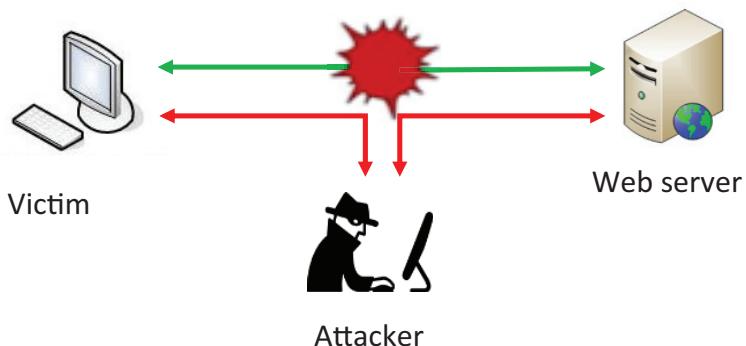


Figure 4.7. MitM attack

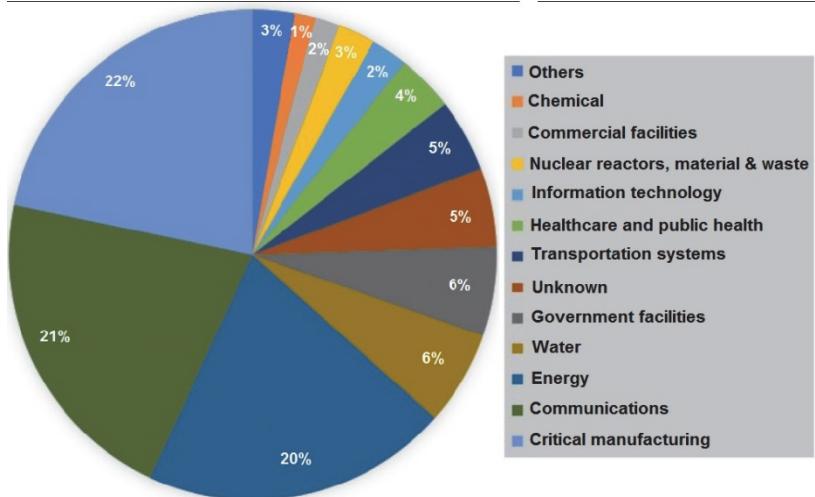


Figure 4.9. *Sectors affected by attacks*

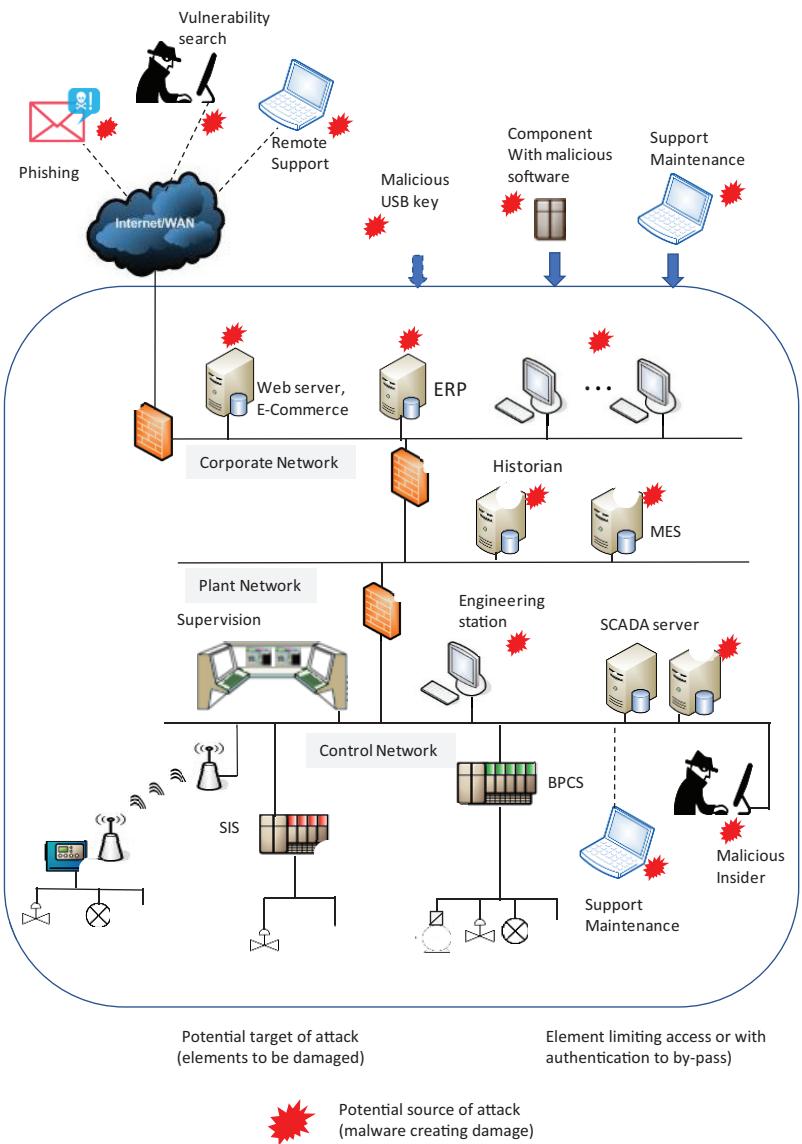


Figure 5.3. Attack surface of an ICS

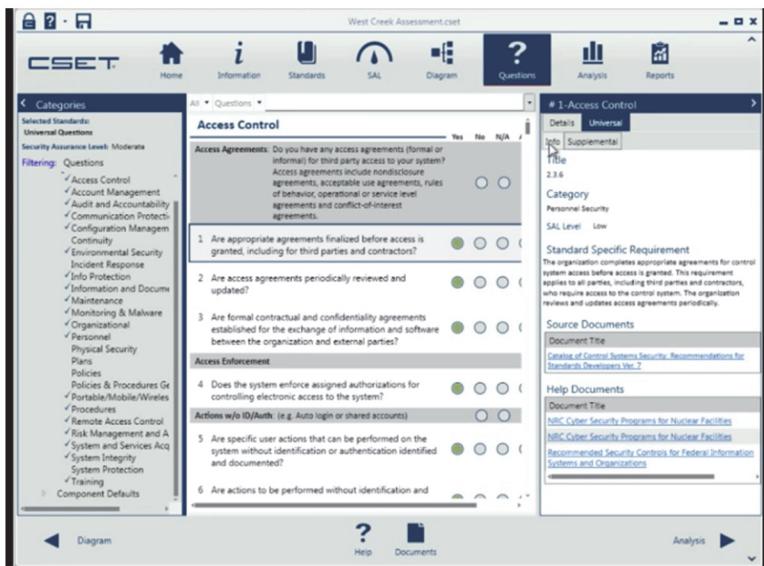


Figure 5.6. Answer to CSET questions screen

The screenshot shows the Greenbone Security Assistant web interface. At the top, there's a navigation bar with links for 'Scan Management', 'Asset Management', 'SeclInfo Management', 'Configuration', 'Extras', 'Administration', and 'Help'. The main content area is titled 'Report: Results' and displays a table of vulnerabilities. The table has columns for 'Vulnerability', 'Severity', 'QoD', 'Host', 'Location', and 'Actions'. The 'Severity' column uses color-coded bars: red for critical, orange for high, yellow for medium, and green for low. The 'Host' column lists IP addresses like 192.168.111.130. The 'Location' column shows port numbers such as 21/tcp, 22/tcp, 80/tcp, etc. The 'Actions' column contains icons for further management. A search bar at the top of the report page includes filters like 'sort-reverse=severity result_hosts_only=1 min_cvss_base= min_qd'.

Vulnerability	Severity	QoD	Host	Location	Actions		
ProFTPD Multiple Remote Vulnerabilities	18.9 (High)	80%	192.168.111.130	21/tcp			
Possible Backdoor: Ingreslock	18.9 (High)	99%	192.168.111.130	1524/tcp			
ProFTPD Multiple Remote Vulnerabilities	18.8 (High)	80%	192.168.111.130	2121/tcp			
X Server	18.8 (High)	80%	192.168.111.130	6000/tcp			
distcc Remote Code Execution Vulnerability	9.3 (High)	99%	192.168.111.130	3632/tcp			
SSH Brute Force Logins with default Credentials	9.8 (High)	95%	192.168.111.130	22/tcp			
MySQL weak password	9.8 (High)	95%	192.168.111.130	3306/tcp			
PostgreSQL weak password	9.8 (High)	99%	192.168.111.130	5432/tcp			
PostgreSQL Multiple Security Vulnerabilities	9.5 (High)	80%	192.168.111.130	5432/tcp			
vstpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	192.168.111.130	21/tcp			
ProFTPD Server SQL Injection Vulnerability	7.5 (High)	75%	192.168.111.130	21/tcp			
phpMyAdmin Code Injection and XSS Vulnerability	7.5 (High)	75%	192.168.111.130	80/tcp			
phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities	7.5 (High)	75%	192.168.111.130	80/tcp			
phpMyAdmin Configuration File PHP Code Injection Vulnerability	7.5 (High)	75%	192.168.111.130	80/tcp			
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (High)	95%	192.168.111.130	80/tcp			
phpinfo() output accessible	7.5 (High)	80%	192.168.111.130	80/tcp			
ProFTPD Server SQL Injection Vulnerability	7.5 (High)	75%	192.168.111.130	2121/tcp			

Figure 5.7. Example of OpenVAS analysis

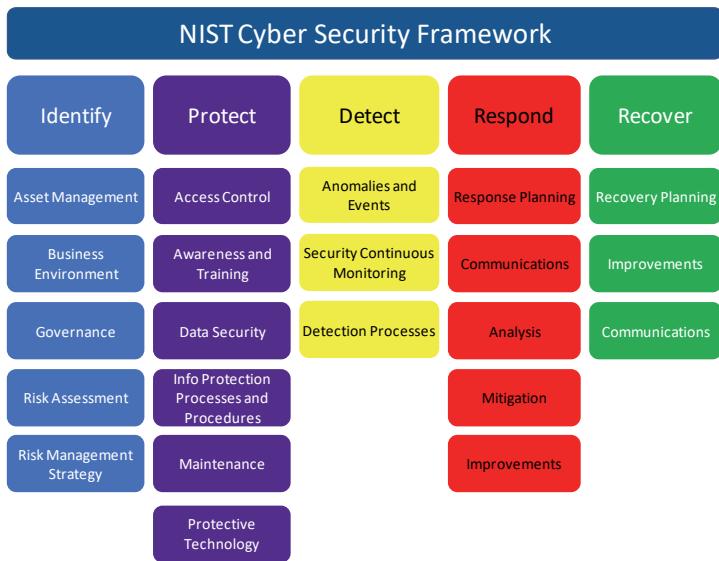


Figure 6.4. *Structure of the NIST framework*

IDENTIFY	ID.AM	Asset Management
	ID.BE	Business Environment
	ID.GV	Governance
	ID.RA	Risk Assessment
	ID.RM	Risk Management Strategy
	ID.SC	Supply Chain Risk Management
PROTECT (PR)	PR.AC	Identity Management, Authentication and Access Control
	PR.AT	Awareness and Training
	PR.DS	Data Security
	PR.IP	Information Protection Processes and Procedures
	PR.MA	Maintenance
	PR.PT	Protective Technology
DETECT (DE)	DE.AE	Anomalies and Events
	DE.CM	Security Continuous Monitoring
	DE.DP	Detection Processes
RESPOND (RS)	RS.RP	Response Planning
	RS.CO	Communications
	RS.AN	Analysis
	RS.MI	Mitigation
	RS.IM	Improvements
RECOVER (RC)	RC.RP	Recovery Planning
	RC.IM	Improvements
	RC.CO	Communications

Figure 6.5. Structure of the NIST Framework

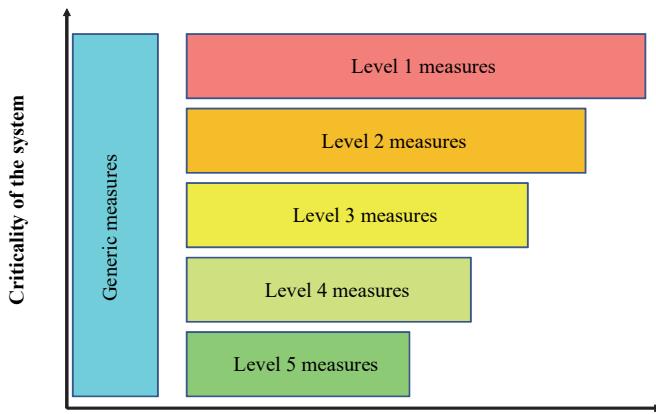


Figure 6.6. Gradual approach

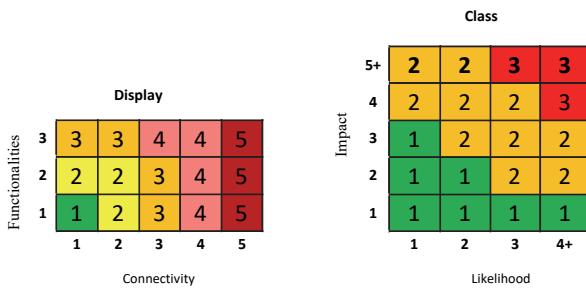


Figure 6.8. Matrix to determine exposure level and class

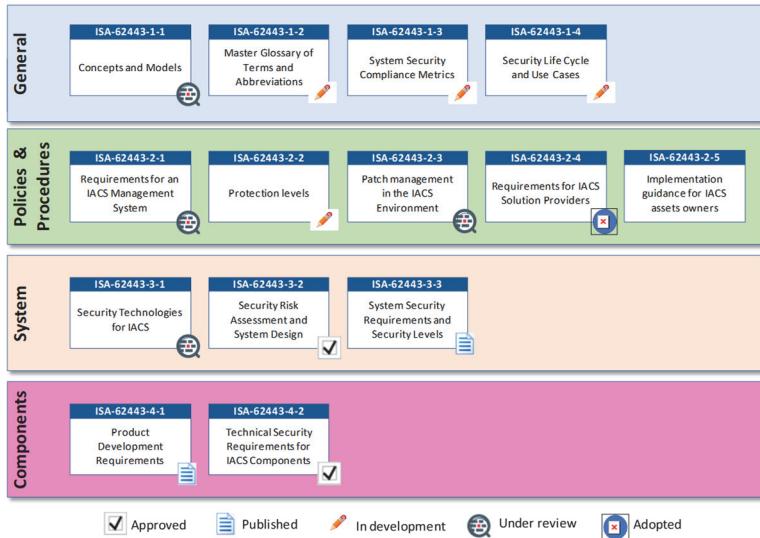


Figure 7.4. Structure of the IEC 62443 (7/2018) standard



Figure 7.7. Security levels

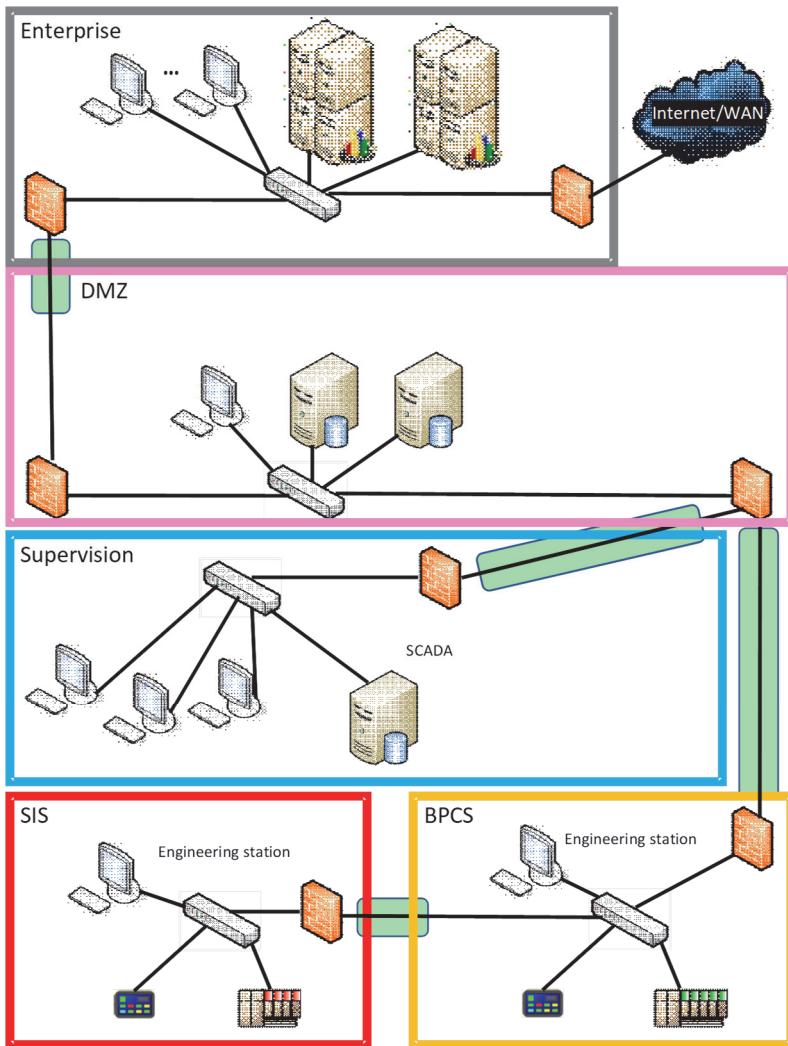


Figure 7.9. Example of division into zones and conduits



Figure 7.10. Maturity levels

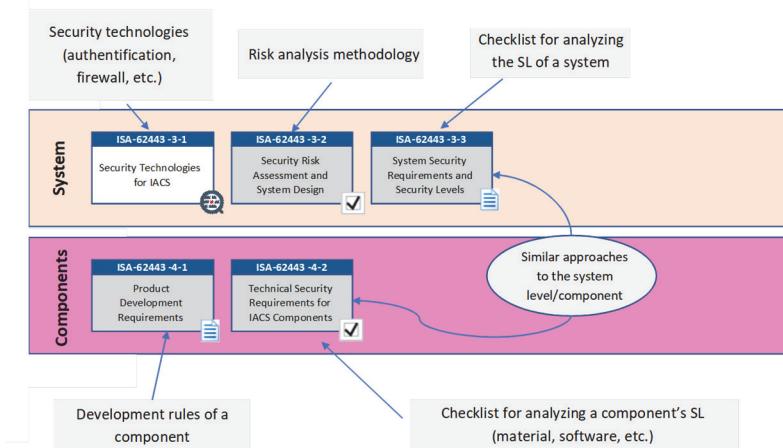


Figure 7.12. Component and system level documents

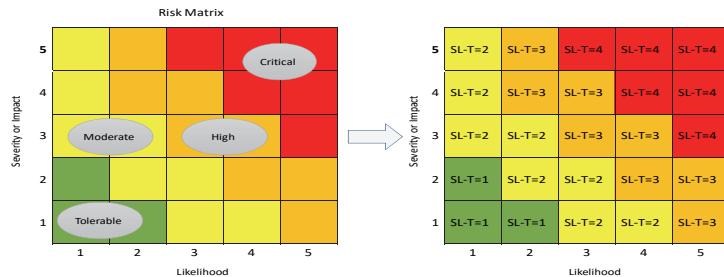


Figure 7.13. Determination of SL-T from the risk matrix

Tolerable Risk=4		
Risk	CRRF	SL-T
1	0,25	0
2	0,5	0
3	0,75	0
4	1	0
5	1,25	1
6	1,5	1
7	1,75	1
8	2	1
9	2,25	2
10	2,5	2
11	2,75	2
12	3	2
13	3,25	3
14	3,5	3
15	3,75	3

Tolerable Risk=4		
Risk	CRRF	SL-T
16	4	3
17	4,25	4
18	4,5	4
19	4,75	4
20	5	4
21	5,25	4
22	5,5	4
23	5,75	4
24	6	4
25	6,25	4

Figure 7.14. Determination of SL-T with CRRF

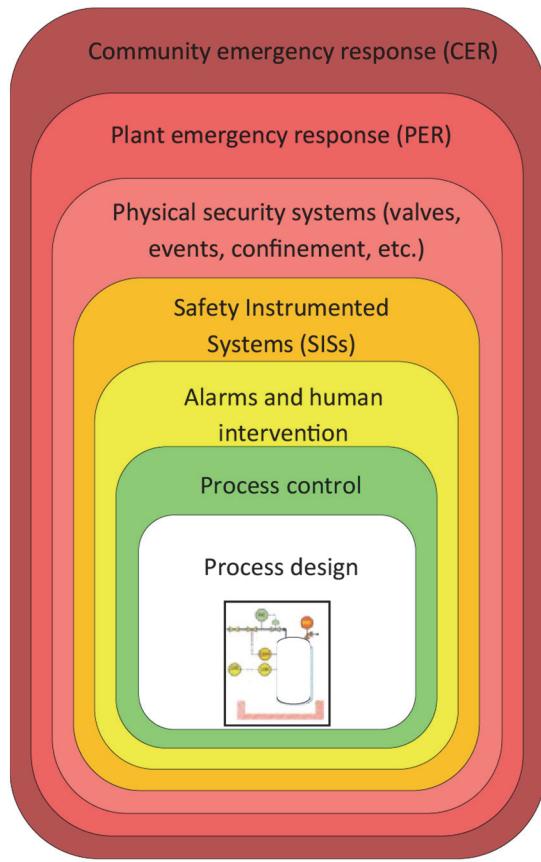


Figure 8.12. Independent Protection Levels (IPL)

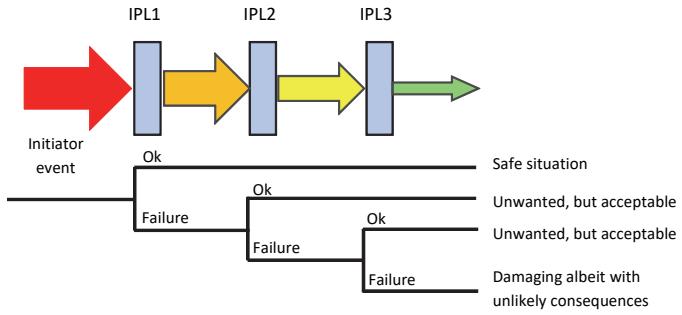


Figure 8.13. IPL and risk management

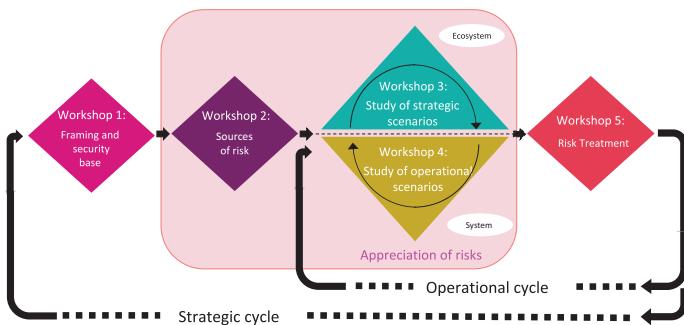


Figure 9.4. Steps of the EBIOS method

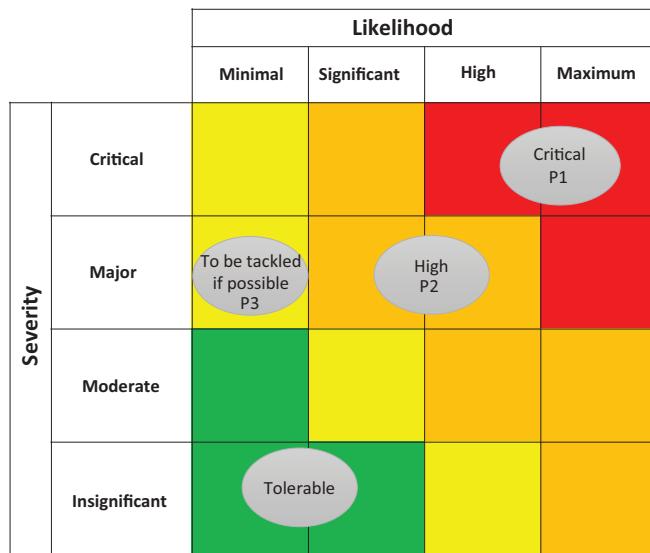


Figure 9.5. Risk matrix

Core assets	Feared event	Security requirement	Impacts	Threat sources	L (likelihood)	S (severity)
Supervision	Tampering of measured data	3. Integrity	Supervision screens out step with real values Uncontrolled production	Internal human source, with malicious intent and limited capabilities External human source, with malicious intent and limited capabilities	3. High	3. Significant

Figure 9.6. Example of an EBIOS analysis table

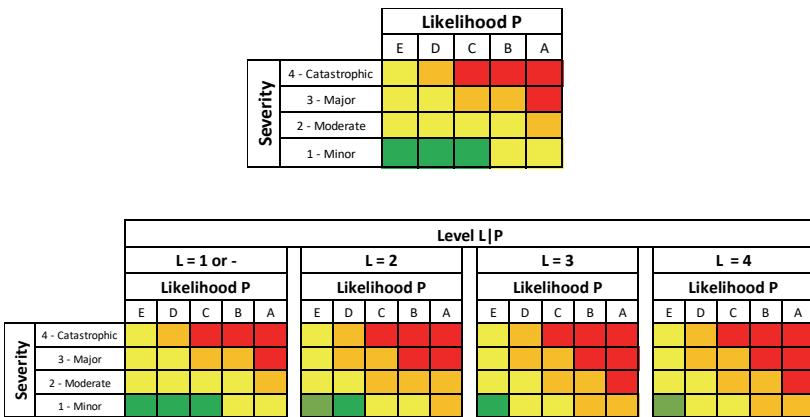


Figure 9.9. Classic risk matrix (top) and scope

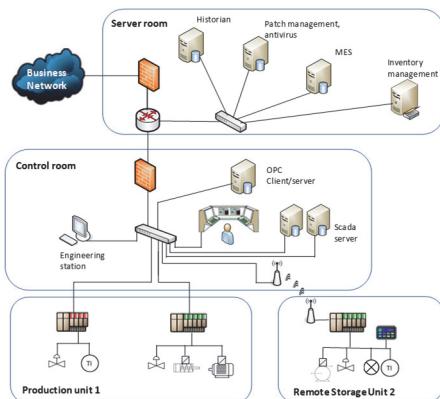


Figure 10.1. Example of physical mapping

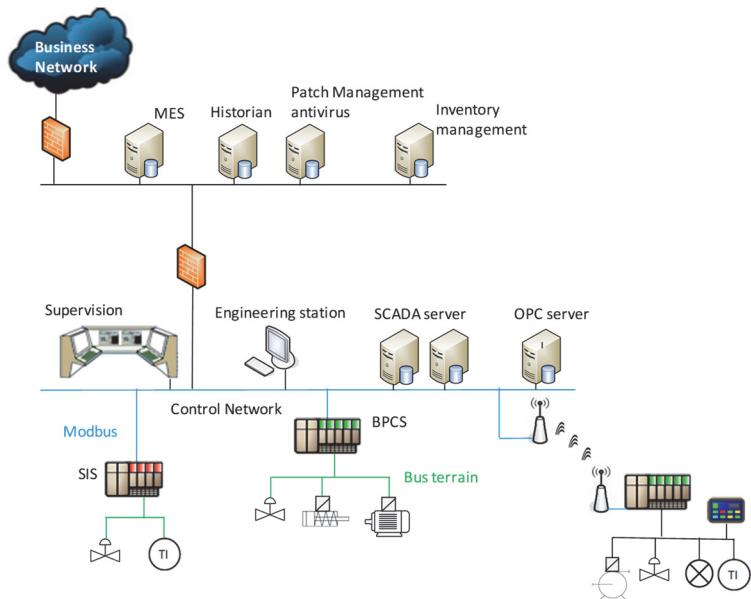


Figure 10.2. Example of logical mapping

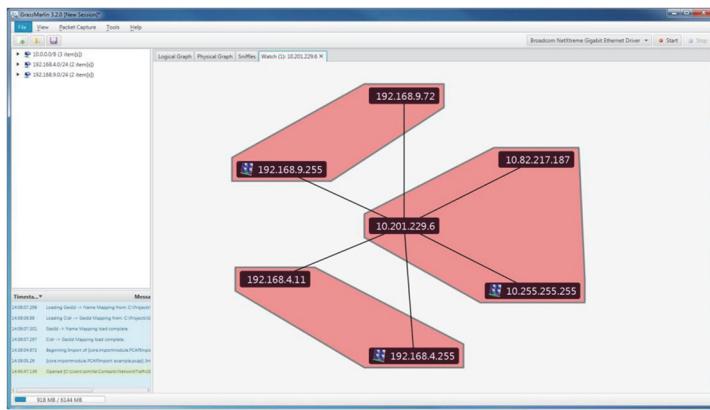


Figure 10.3. Grassmarlin screenshot

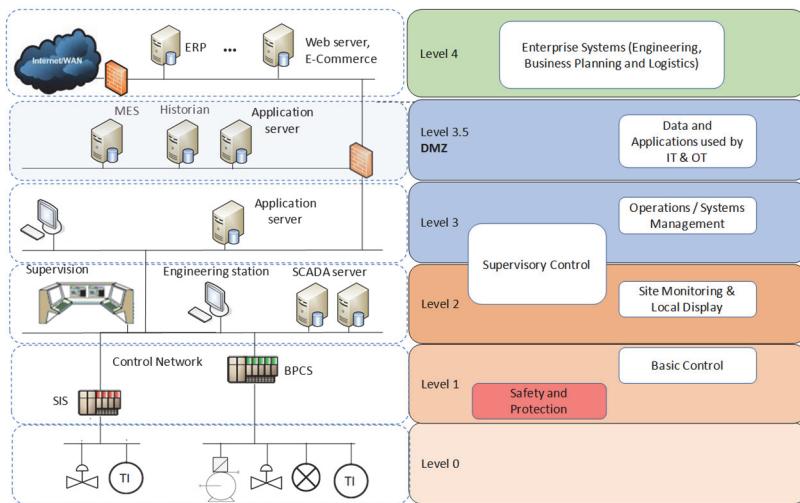


Figure 10.4. Architecture with a DMZ

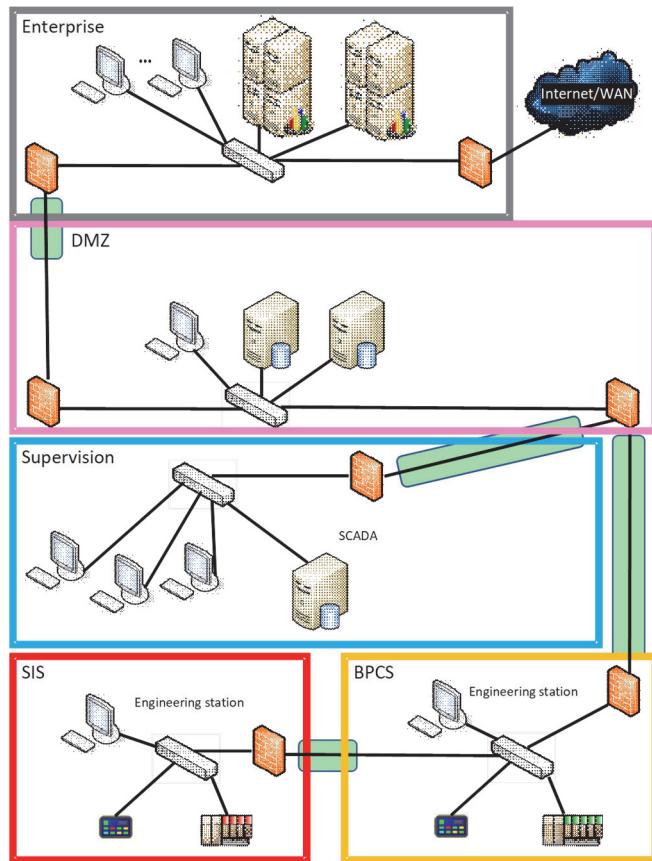


Figure 10.5. Example of division into zones and conduits

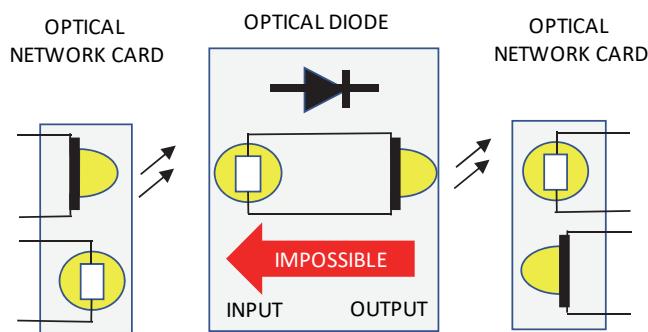


Figure 10.6. Principle of a data diode

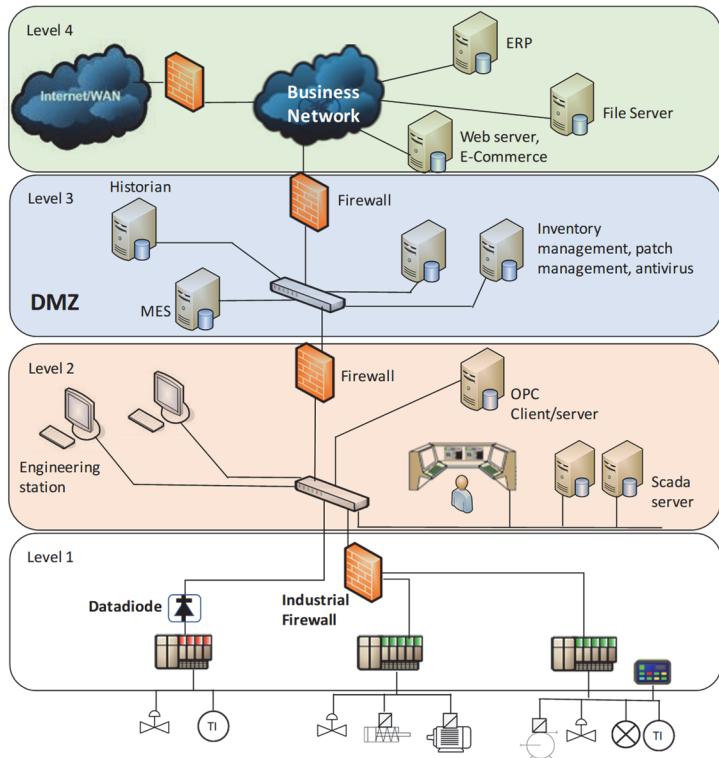


Figure 10.7. Example of an architecture with data diode, firewall and industrial firewall

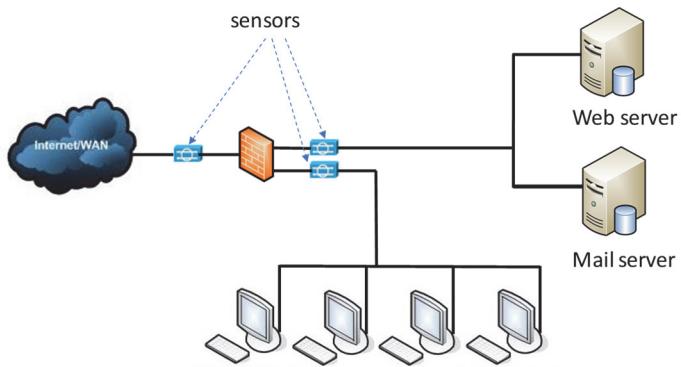


Figure 10.8. NIDS

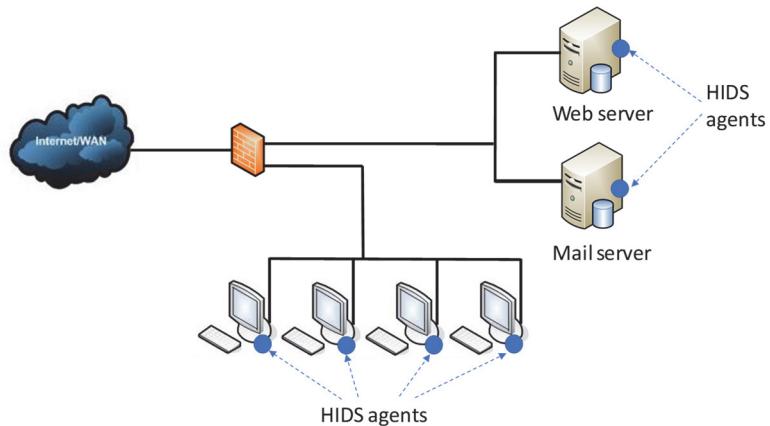


Figure 10.9. HIDS

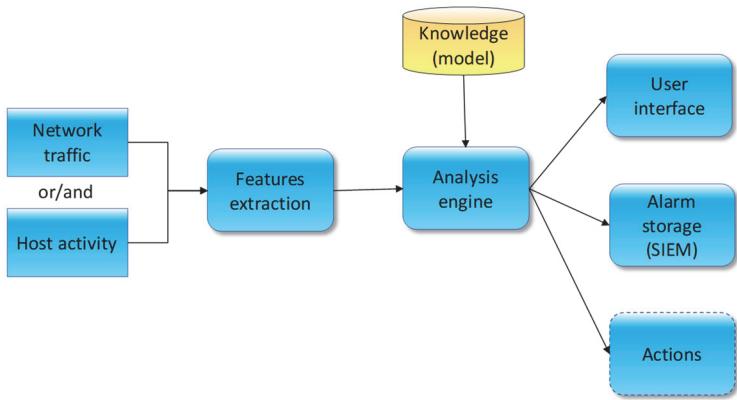


Figure 10.10. Structure of an IDS

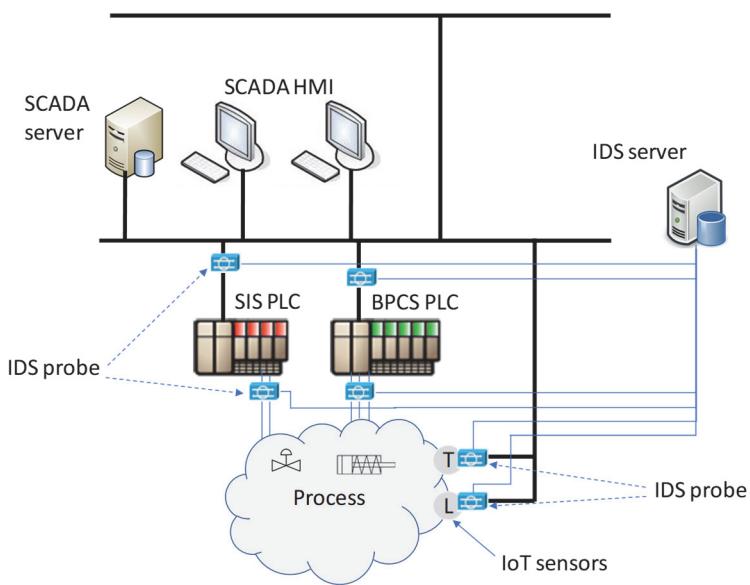


Figure 10.11. Structure of an industrial IDS

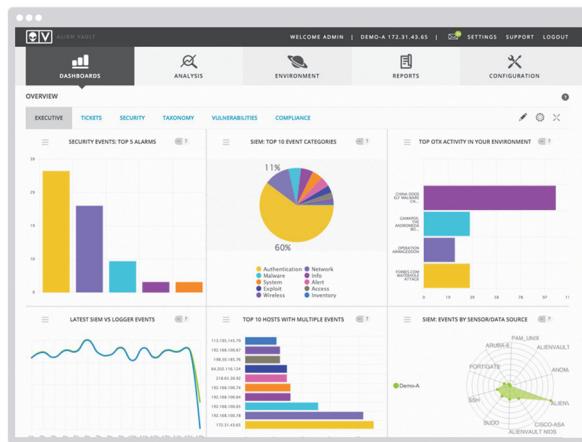


Figure 10.12. SIEM screen

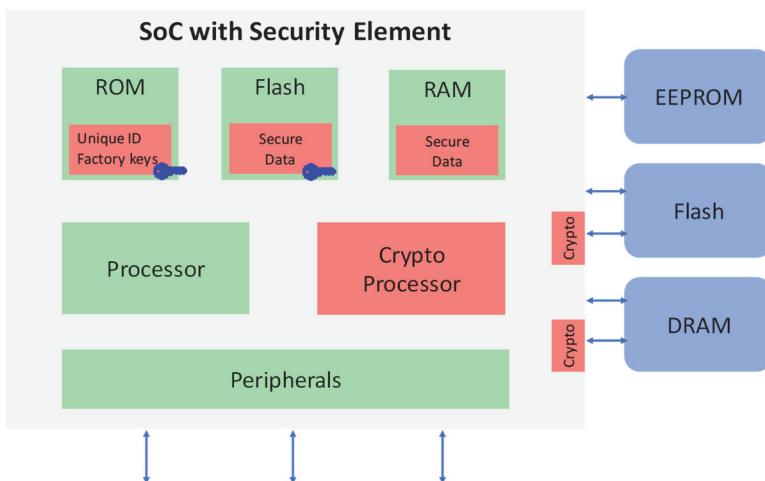


Figure 10.13. SoC with security element

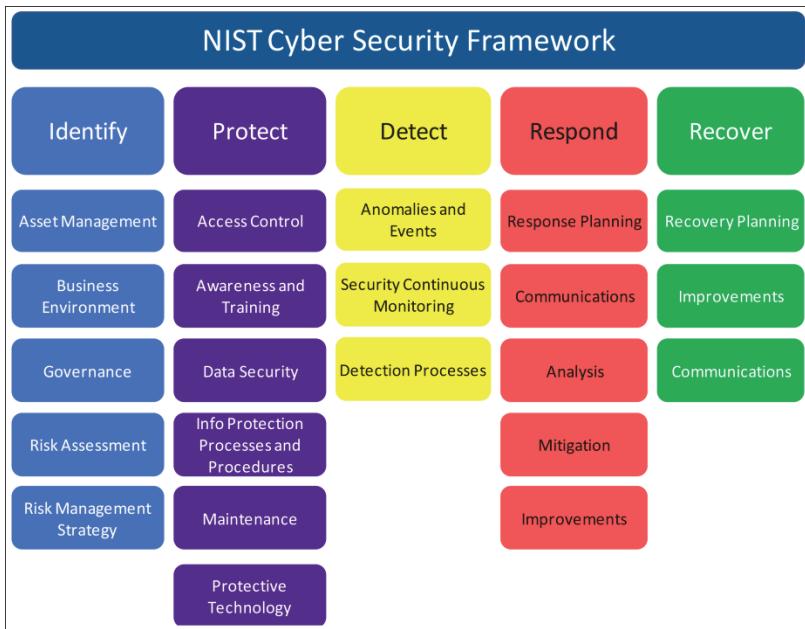


Figure 11.1. Structure of the NIST framework

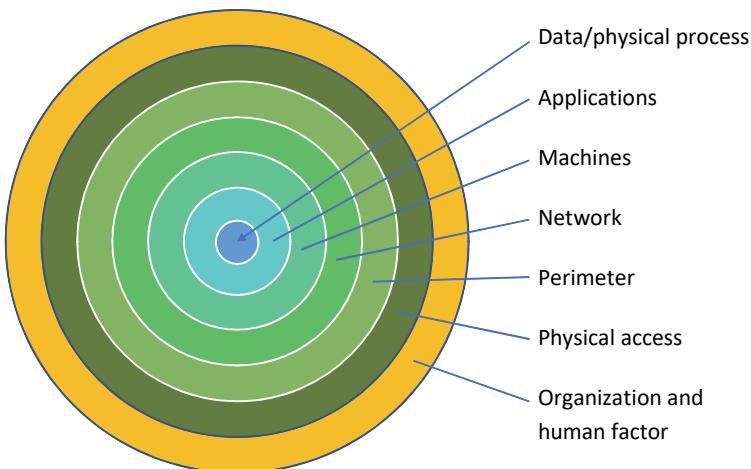


Figure 11.2. Defense in depth

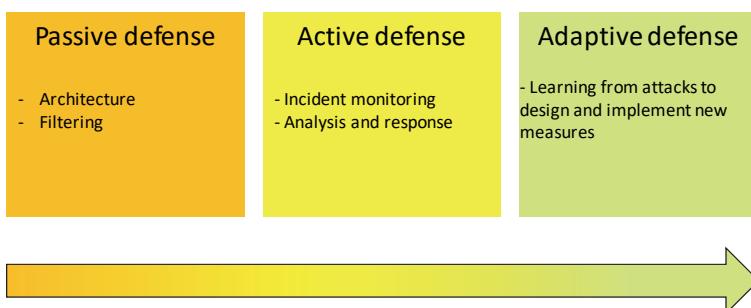


Figure 11.3. Different levels of countermeasures

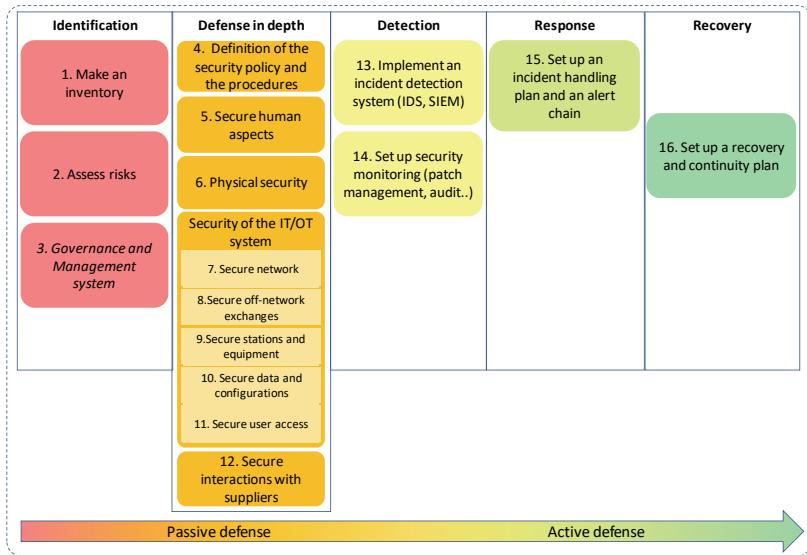


Figure 11.4. Steps in the ICS security process