FHI INDUSTRIËLE AUTOMATISERING

How to use the NIST framework to start your cyber security journey.

Productie Proces Automatisering

24 januari 2023 | Hart van Holland Nijkerk

Life Is On Schneider Electric

FHI INDUSTRIËLE AUTOMATISERING

Geoffroy Moens

Cybersecurity Architect
Schneider Electric

The NIST Cybersecurity Framework

Three Primary Components

National Institute of Standards and Technology
U.S. Department of Commerce

Core

Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls

Profiles

Alignment of an organization's requirements and objectives, risk appetite and resources ***using*** the desired outcomes of the Framework Core

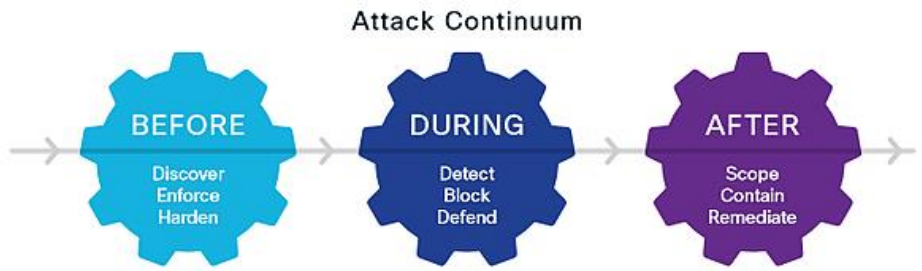
Implementation Tiers

A qualitative measure of organizational cybersecurity risk management practices

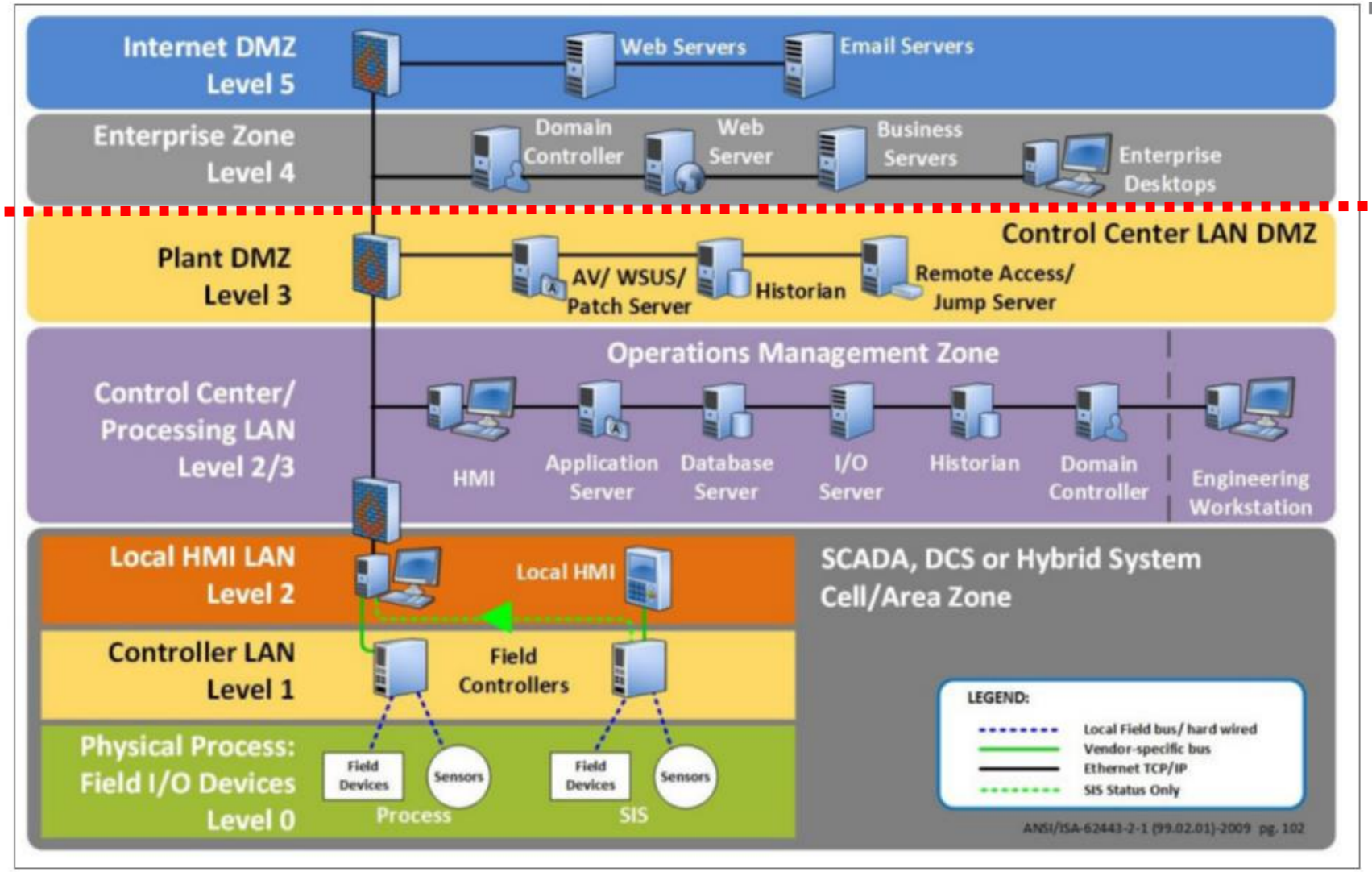
Key Framework Attributes

Principles of Current and Future Versions of the Framework

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Living document
- Guided by many perspectives – private sector, academia, public sector

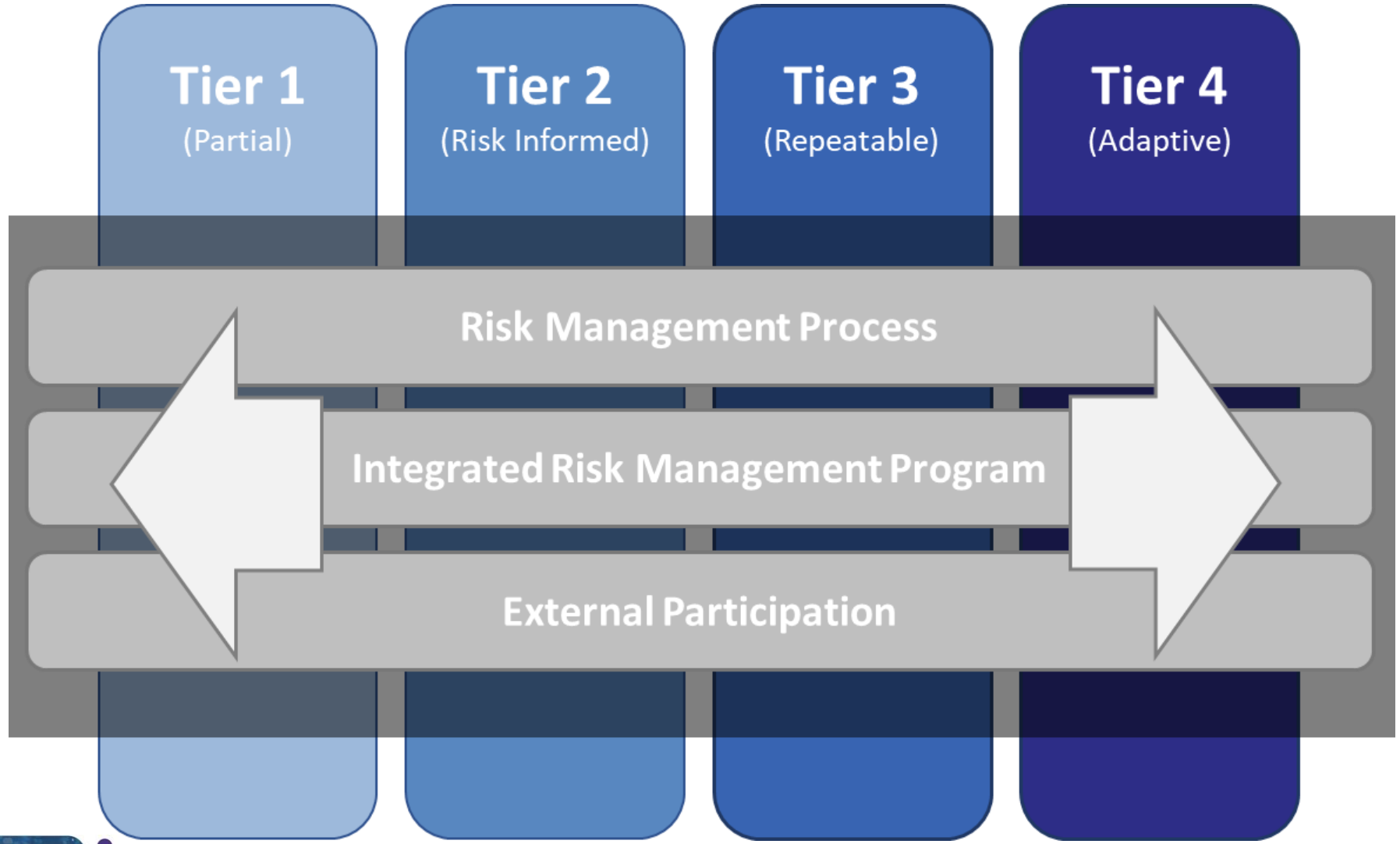


The NIST Framework vs Standards



Implementation Tiers

The Cybersecurity Framework Version 1.1



The Framework Core

	Function	Category	ID
What processes and assets need protection?	Identify	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
		Supply Chain Risk Management	ID.SC
What safeguards are available?	Protect	Identity Management & Access Control	PR.AC
		Awareness and Training	PR.AT
		Data Security	PR.DS
		Information Protection Processes & Procedures	PR.IP
		Maintenance	PR.MA
		Protective Technology	PR.PT
What techniques can identify incidents?	Detect	Anomalies and Events	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
What techniques can contain impacts of incidents?	Respond	Response Planning	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements	RS.IM
What techniques can restore capabilities?	Recover	Recovery Planning	RC.RP
		Improvements	RC.IM
		Communications	RC.CO

The Framework Core

A translation layer

Senior Executives

- Broad enterprise considerations
- Abstracted risk vocabulary

Specialists in Other Fields

- Specific focus outside of cybersecurity
- Specialized or no risk vocabulary

Implementation / Operations

- Deep technical considerations
- Highly specialized vocabulary

FHI INDUSTRIËLE AUTOMATISERING

The Framework Core

5 Functions 23 Categories

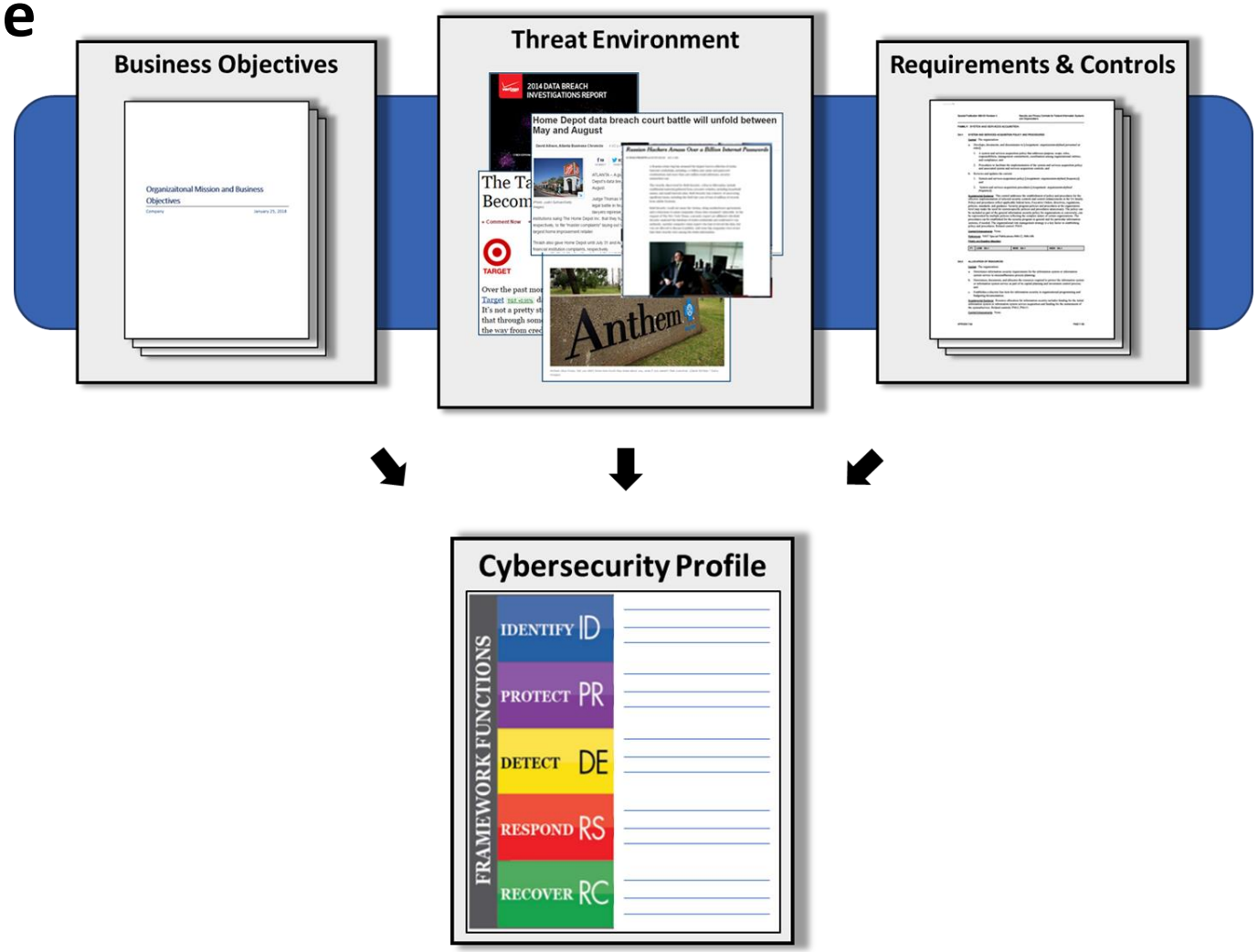
Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management & Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

108 Subcategories 6 Informative References

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

The Framework Profile

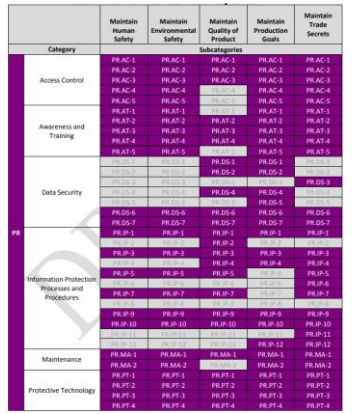
- Alignment with business requirements, risk tolerance, and organizational resources
- Enables organizations to establish a roadmap for reducing cybersecurity risk
- Used to describe current state or desired target state of cybersecurity activities

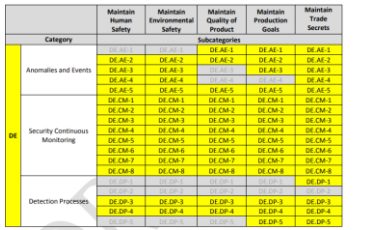


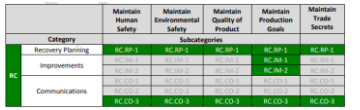
The Framework Profile

IDENTIFY Business Mission Objectives

		Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Product	Maintain Production Goals	Maintain Trade Secrets
	Category	**Subcategories**				
ID	Asset Management	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1
		ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2
		ID.AM-3	ID.AM-3	ID.AM-3	ID.AM-3	ID.AM-3
		ID.AM-4	ID.AM-4	ID.AM-4	ID.AM-4	ID.AM-4
		ID.AM-5	ID.AM-5	ID.AM-5	ID.AM-5	ID.AM-5
		ID.AM-6	ID.AM-6	ID.AM-6	ID.AM-6	ID.AM-6
	Business Environment	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1
		ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2
		ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3
		ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4
		ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5
	Governance	ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1
		ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2
		ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3
		ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4
	Risk Assessment	ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1
		ID.RA-2	ID.RA-2	ID.RA-2	ID.RA-2	ID.RA-2
		ID.RA-3	ID.RA-3	ID.RA-3	ID.RA-3	ID.RA-3
		ID.RA-4	ID.RA-4	ID.RA-4	ID.RA-4	ID.RA-4
		ID.RA-5	ID.RA-5	ID.RA-5	ID.RA-5	ID.RA-5
		ID.RA-6	ID.RA-6	ID.RA-6	ID.RA-6	ID.RA-6
	Risk Management Strategy	ID.RM-1	ID.RM-1	ID.RM-1	ID.RM-1	ID.RM-1
		ID.RM-2	ID.RM-2	ID.RM-2	ID.RM-2	ID.RM-2
		ID.RM-3	ID.RM-3	ID.RM-3	ID.RM-3	ID.RM-3







The Framework Profile

The Security levels for Manufacturing

- The potential impact is LOW if the loss of integrity, availability, or confidentiality could be expected to have a limited adverse effect on manufacturing operations, assets, personnel, the general public, or the environment.
- The potential impact is **MODERATE** if the loss of integrity, availability, or confidentiality could be expected to have a serious adverse effect on manufacturing operations, assets, personnel, the general public, or the environment.
- The potential impact is **HIGH** if the loss of integrity, availability, or confidentiality could be expected to have a severe or catastrophic adverse effect on manufacturing operations, assets, personnel, the general public, or the environment.

Impact Category	Low-Impact	Moderate-Impact	High-Impact
Injury	Cuts, bruises requiring first aid	Requires hospitalization	Loss of life or limb
Financial Loss	$1,000	$100,000	Millions
Environmental Release	Temporary damage	Lasting damage	Permanent damage, off-site damage
Interruption of Production	Minutes	Days	Weeks
Public Image	Temporary damage	Lasting damage	Permanent damage

FHI INDUSTRIËLE AUTOMATISERING

The Framework Profile

Examples of Security levels

Function	Category	Subcategory	Manufacturing Profile	Reference
IDENTIFY	ID.AM	ID.AM-1	**Low**	62443-2-1:2009 4.2.3.4 62443-3-3:2013 SR 7.8
			Document an inventory of manufacturing system components that reflects the current system. Manufacturing system components include for example PLCs, sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices. System component inventory is reviewed and updated as defined by the organization. Information deemed necessary for effective accountability of manufacturing system components includes, for example, hardware inventory specifications, component owners, networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.	CM-8
			Moderate	
			Employ automated mechanisms where feasible to detect the presence of unauthorized hardware and firmware components within the system.	CM-8 (1)(3)(5)
			High	
			Identify individuals who are both responsible and accountable for administering manufacturing system components.	CM-8 (2)(4)

The Framework Profile

Examples of Security levels

Function	Category	Subcategory	Manufacturing Profile	Reference
		PR.AC-3	**Low**	62443-2-1:2009 4.3.3.6.6 62443-3-3:2013 SR 1.13,2.6
			Establish usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the manufacturing system. Provide an explicit indication of active remote access connections to users physically present at the devices. Remote access methods include, for example, wireless, dial-up, broadband, VPN connections, mobile device connections, and communications through external networks.	AC-17,19,20 SC-15
			Moderate and High	
			Allow remote access only through approved and managed access points. Monitor remote access to the manufacturing system, and employ cryptographic mechanisms where determined necessary. Allow only authorized use of privileged functions from remote access. Establish agreements and verify security for connections with external systems.	AC-17(1)(2)(3)(4) AC-20(1)(2)

FHI INDUSTRIËLE AUTOMATISERING

The Framework Profile

Examples of Security levels

Function	Category	Subcategory	Manufacturing Profile	Reference
DETECT	DE.CM	DE.CM-1	**Low**	62443-3-3:2013 SR 6.2
			Conduct ongoing security status monitoring of the manufacturing system network to detect attacks and indicators of potential attacks.	CA-7d AC-2g,
			Detect unauthorized local, network, and remote connections, and identify unauthorized use of the manufacturing system.	SI-4b
			Generate audit records for defined cybersecurity events.	AU-12c
			Monitor network communications at the external boundary of the system and at key internal boundaries within the system.	SC-7, SI-4(4)
			Heighten system monitoring activity whenever there is an indication of increased risk.	SI-4e
			Moderate	
			Employ automated mechanisms to support detection of cybersecurity events.	AC-2 (1)(2)(3)(4), SI-4(2)
			Generate system alerts when indications of compromise or potential compromise occur.	SI-4(5)
			High	
			Monitor for and report atypical usage of the manufacturing system.	AC-2(12)

The Framework Profile

Examples of Security levels

Function	Category	Subcategory	Manufacturing Profile	Reference
RESPOND		RS.CO-2	**Low**	62443-2-1:2009 4.3.4.5.5
			Employ prompt reporting to appropriate stakeholders for cybersecurity events on the manufacturing system.	IR-6,
			Ensure that cybersecurity events on the manufacturing system are reported consistent with the response plan.	AU-6
			Moderate and High	
			Employ automated mechanisms to assist in the reporting of cybersecurity events.	IR-6(1)

Function	Category	Subcategory	Manufacturing Profile	Reference
	RC.RP	RC.RP-1	**Low and Moderate**	
			Execute the recovery plan during or after a cybersecurity incident on the manufacturing system.	IR-8, CP-10
			Restore the manufacturing system within a predefined time-period from configuration-controlled and integrity-protected information representing a known, operational state for the components.	CP-10(4)
			High	
			Continue essential manufacturing functions and services with little or no loss of operational continuity, and sustain continuity until full system restoration.	CP-2(5)

Sample Resources

www.nist.gov/cyberframework/framework-documents

Manufacturing Profile

NIST Discrete Manufacturing Cybersecurity Framework Profile

Smart GRID Profile

Cybersecurity Framework
Smart Grid Profile

Maritime Profile

Bulk Liquid Transport Profile

FHI INDUSTRIËLE AUTOMATISERING

? Q&A

FHI INDUSTRIËLE AUTOMATISERING

Thank You

- More info at the Schneider Electric booth

Bert Poort
Business Development Manager
bert.poort@se.com