UN CRO Guidelines for Cybersecurity update

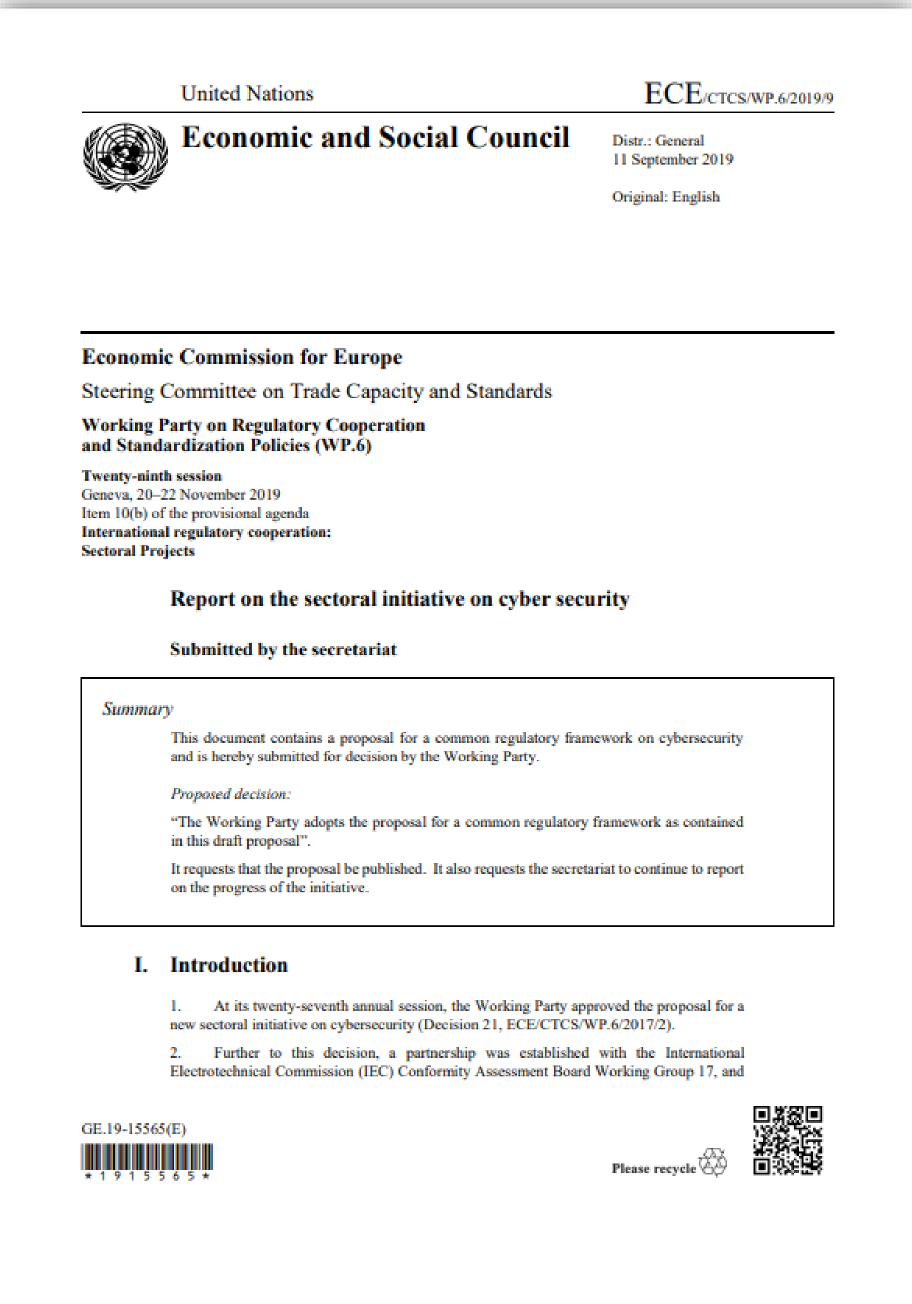
David Hanlon

Secretary, IEC Conformity Assessment Board (CAB)

UNECE WP.6 GRM plenary
UNOG, Geneva - remote
9th June, 2022

International
Electrotechnical
Commission

UN CRO Guidelines for Cybersecurity



United Nations

ECE/CTCS/WP.6/2019/9

Economic and Social Council

Distr.: General
11 September 2019

Original: English

Economic Commission for Europe

Steering Committee on Trade Capacity and Standards

Working Party on Regulatory Cooperation and Standardization Policies (WP.6)

Twenty-ninth session
Geneva, 20–22 November 2019
Item 10(b) of the provisional agenda
International regulatory cooperation:
Sectoral Projects

Report on the sectoral initiative on cyber security

Submitted by the secretariat

Summary

This document contains a proposal for a common regulatory framework on cybersecurity and is hereby submitted for decision by the Working Party.

Proposed decision:

"The Working Party adopts the proposal for a common regulatory framework as contained in this draft proposal".

It requests that the proposal be published. It also requests the secretariat to continue to report on the progress of the initiative.

I. Introduction

1. At its twenty-seventh annual session, the Working Party approved the proposal for a new sectoral initiative on cybersecurity (Decision 21, ECE/CTCS/WP.6/2017/2).

2. Further to this decision, a partnership was established with the International Electrotechnical Commission (IEC) Conformity Assessment Board Working Group 17, and

GE.19-15565(E)

1915565

Please recycle

- Development started in 2017
- Draft version endorsed in November 2018
- Further developed during 2019
- Sector examples added in 2019
- Final version approved in November 2019

- A living document

Published CRO available here…

http://www.unece.org/tradewelcome/tradewp6/groups/cybersecurity.html

Systematic Methodology

Systems-approach

- Model the system
- Use the GMM
- Risk-based
- Open choice of requirements

  → could be standards based

  → open choice of standards

- Open choice of conformity assessment (CA)

  Use appropriate CA at appropriate points according to risk.

  → suppliers declaration (1st party)

  → Internal audits (2nd party)

  → Certification (3rd party)

Systematic Methodology

Systems-approach

- Model the system
- Use the GMM
- Risk based
- Open choice of requirements

  → could be standards based

  → open choice of standards

- Open choice of conformity assessment (CA)

  Use appropriate CA at appropriate points according to risk.

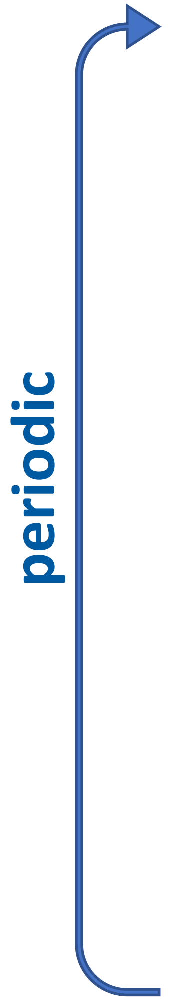
  → suppliers declaration (1st party)

  → Internal audits (2nd party)

  → Certification (3rd party)

Often forgotten in other frameworks, yet essential

Systematic Methodology



1) Map sector application to Generic Matrix Model (GMM)
2) Risk analysis of sector application map
   - Identify and rate risk points
3) Determine appropriate level of CA for each risk point according to risk level rating
4) Identify requirements documents (standards)
   - Determine what is available/appropriate
     → standards gap analysis
   - Determine how to fill the gaps (→ standards development)
5) Apply appropriate CA to appropriate standards at each risk point

Revue, revise, renew (R3)

Systematic Methodology

Generic Matrix Model (GMM)

SYSTEM MODEL

Components

product A, B, C…
Product development
Product manufacture
etc

Interconnections

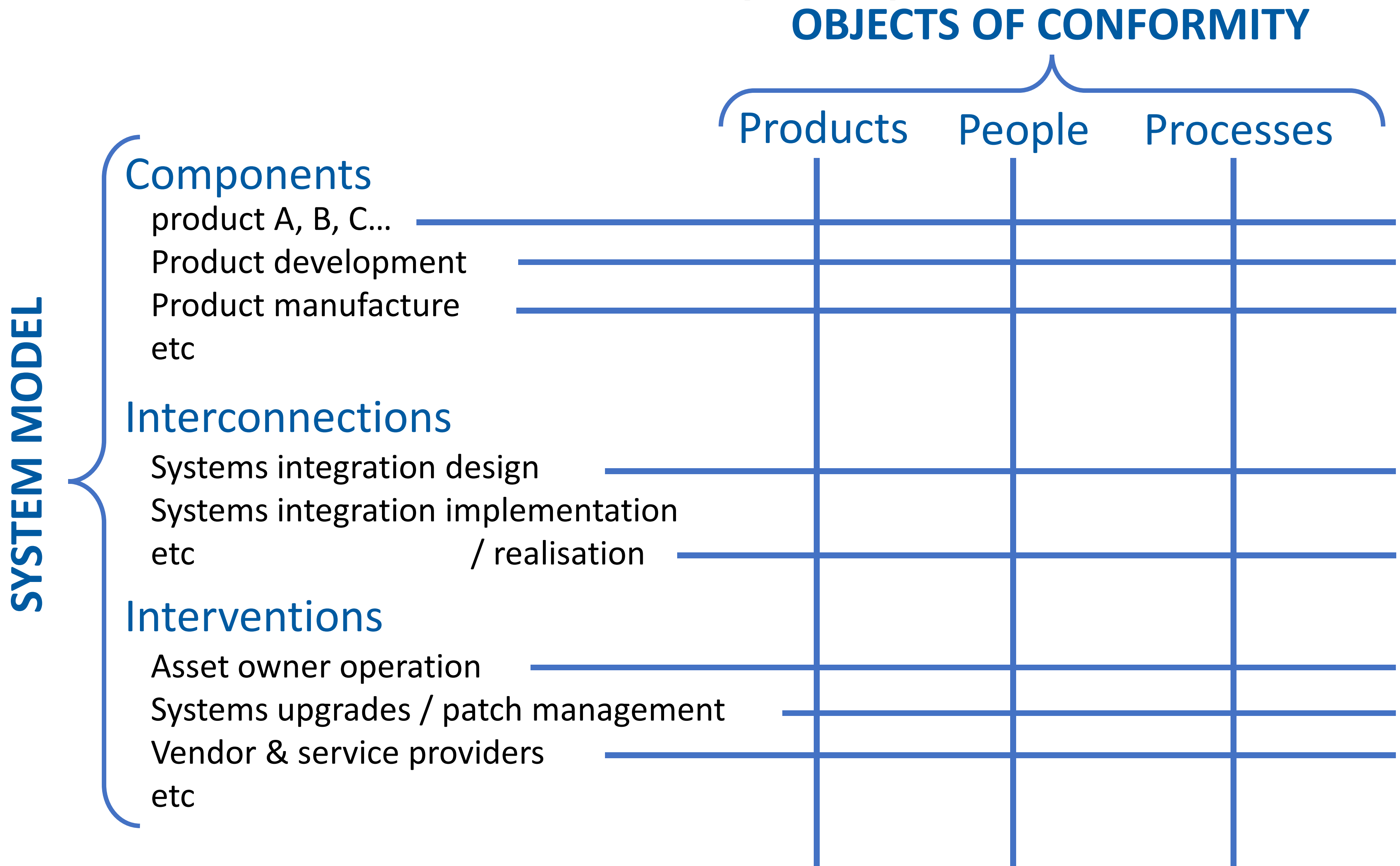
Systems integration design
Systems integration implementation
etc / realisation

Interventions

Asset owner operation
Systems upgrades / patch management
Vendor & service providers
etc

Systematic Methodology

Generic Matrix Model (GMM)



OBJECTS OF CONFORMITY

Products

People

Processes

SYSTEM MODEL

Components

product A, B, C…

Product development

Product manufacture

etc

Interconnections

Systems integration design

Systems integration implementation

etc / realisation

Interventions

Asset owner operation

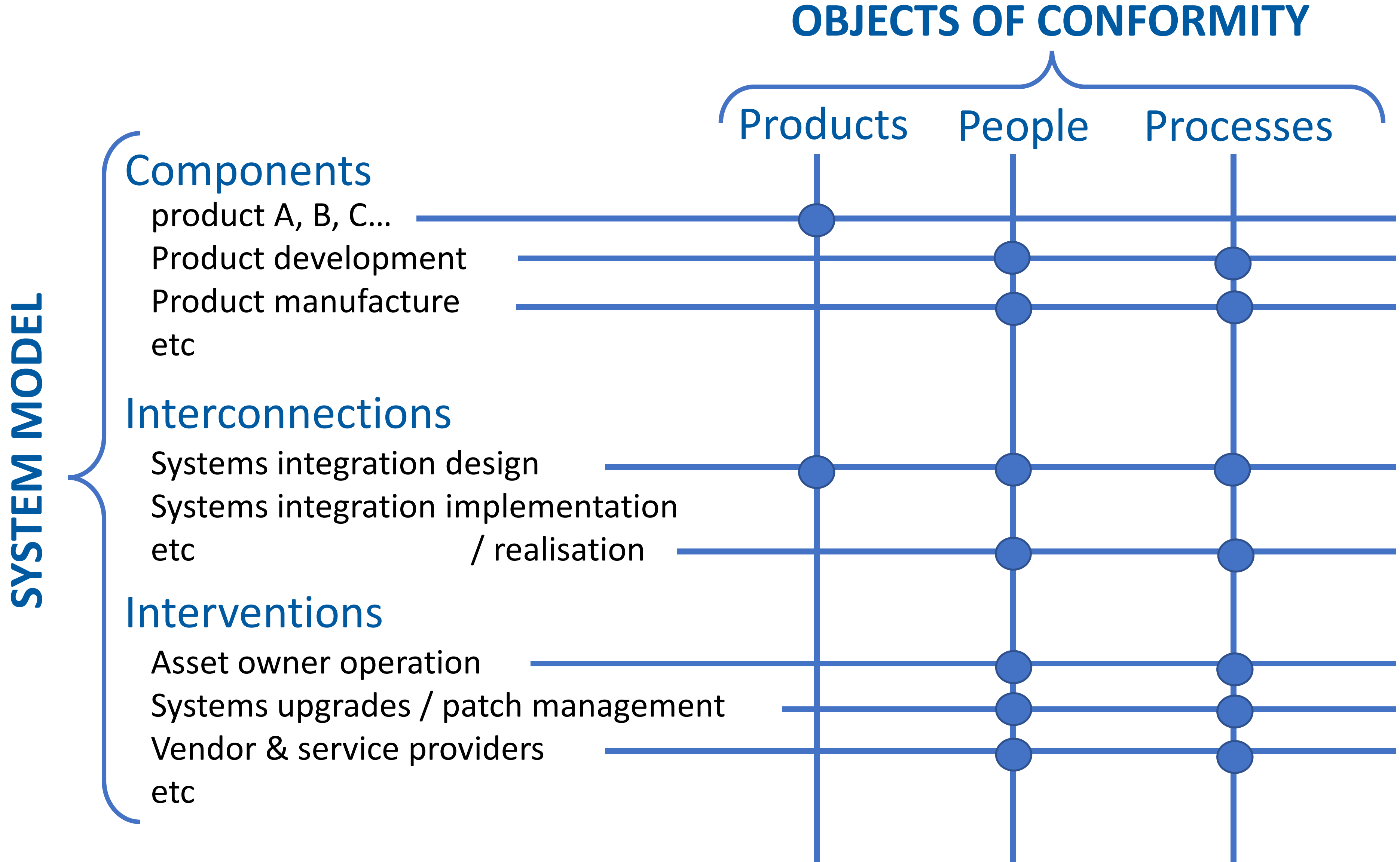
Systems upgrades / patch management

Vendor & service providers

etc

Systematic Methodology

Generic Matrix Model (GMM)



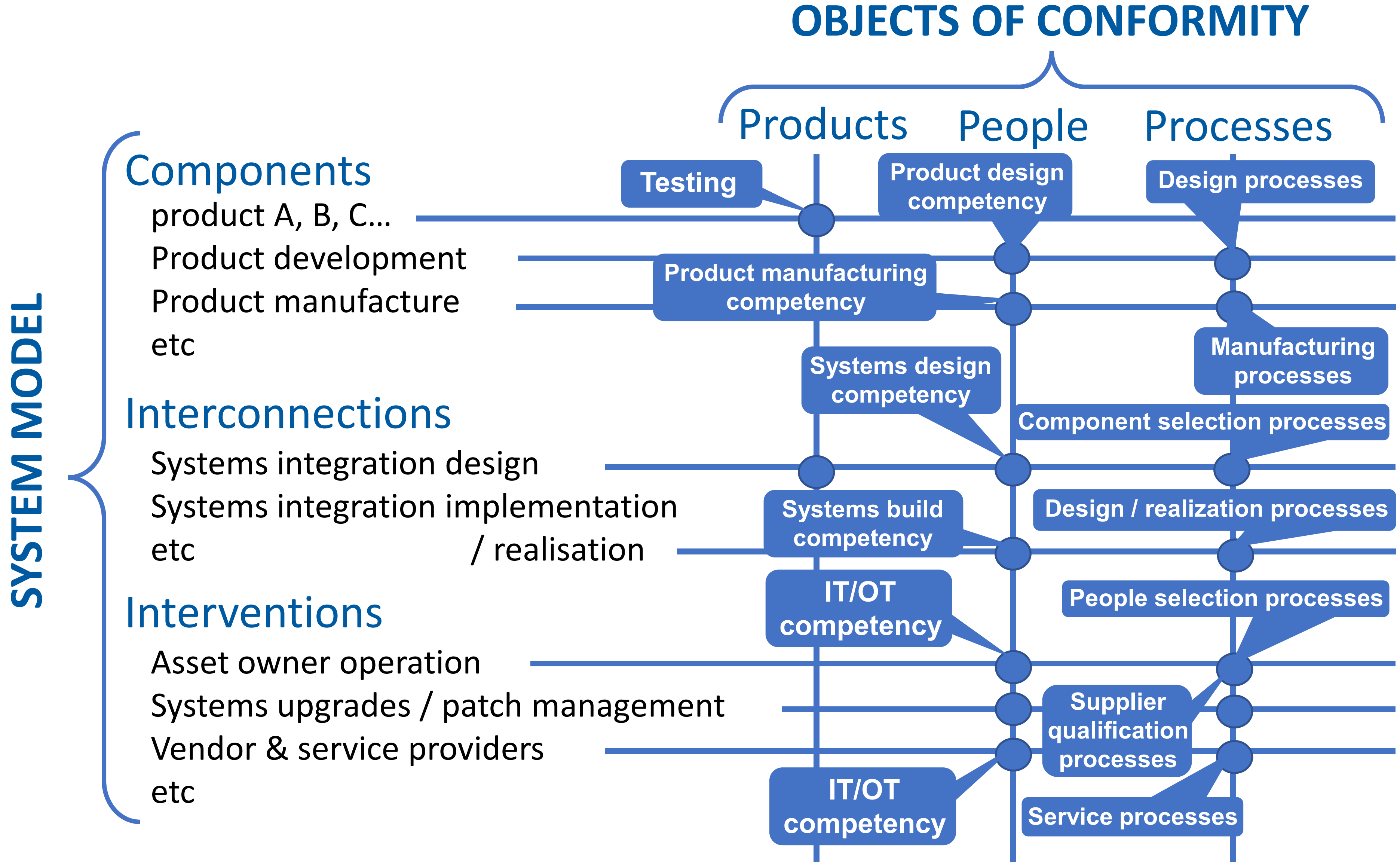
OBJECTS OF CONFORMITY

SYSTEM MODEL

	Products	People	Processes
Components			
product A, B, C…	●		
Product development		●	●
Product manufacture		●	●
etc			
Interconnections			
Systems integration design	●	●	●
Systems integration implementation / realisation		●	●
etc			
Interventions			
Asset owner operation		●	●
Systems upgrades / patch management		●	●
Vendor & service providers		●	●
etc			

Systematic Methodology

Generic Matrix Model (GMM)



OBJECTS OF CONFORMITY

Products People Processes

SYSTEM MODEL

Components
- product A, B, C…
- Product development
- Product manufacture
- etc

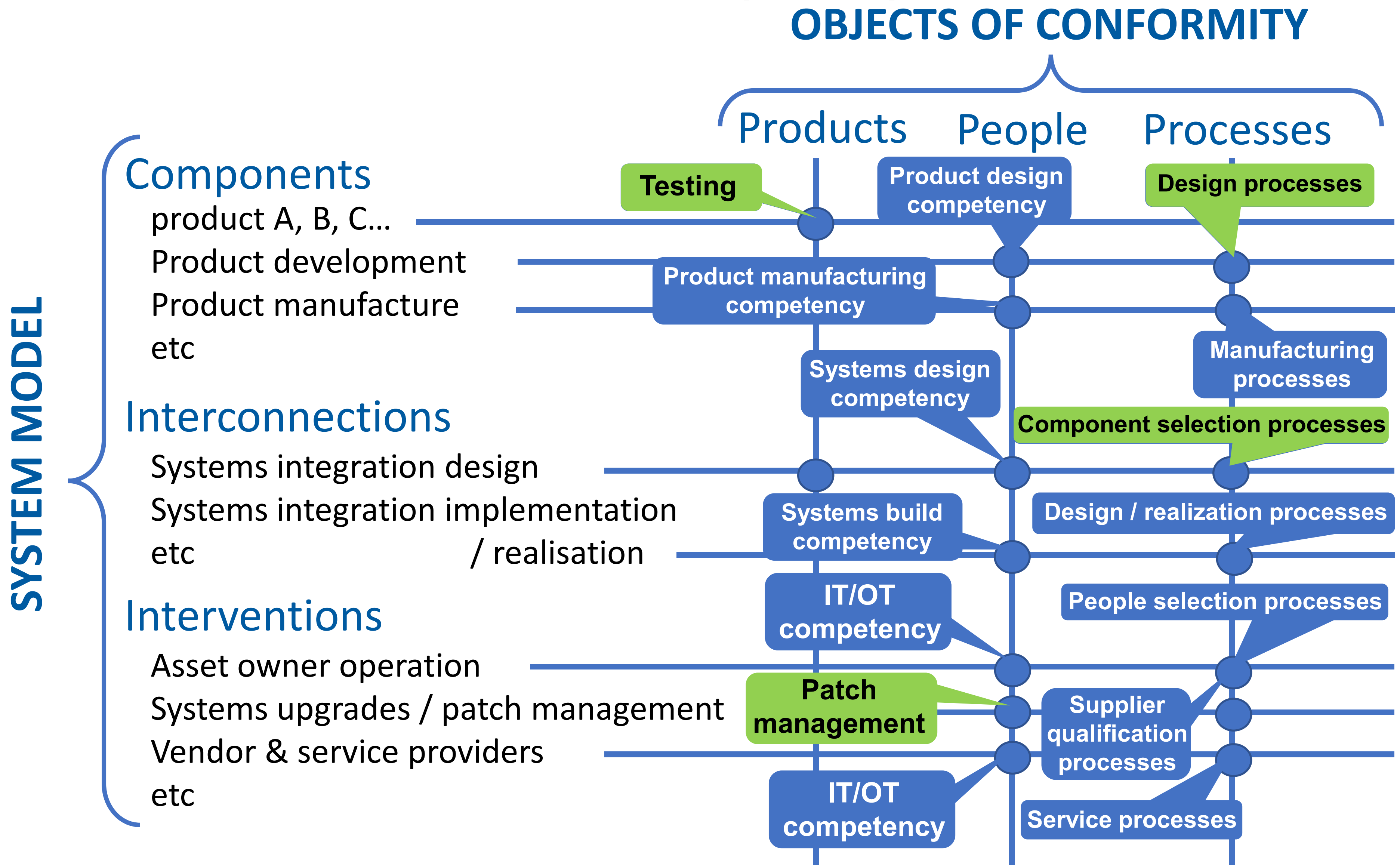
Interconnections
- Systems integration design
- Systems integration implementation / realisation
- etc

Interventions
- Asset owner operation
- Systems upgrades / patch management
- Vendor & service providers
- etc

Testing
Product design competency
Design processes
Product manufacturing competency
Manufacturing processes
Systems design competency
Component selection processes
Systems build competency
Design / realization processes
IT/OT competency
People selection processes
Supplier qualification processes
IT/OT competency
Service processes

Systematic Methodology

Generic Matrix Model (GMM)



OBJECTS OF CONFORMITY

Products

People

Processes

SYSTEM MODEL

Components

product A, B, C…

Product development

Product manufacture

etc

Interconnections

Systems integration design

Systems integration implementation

etc / realisation

Interventions

Asset owner operation

Systems upgrades / patch management

Vendor & service providers

etc

Testing

Product design competency

Design processes

Product manufacturing competency

Manufacturing processes

Systems design competency

Component selection processes

Systems build competency

Design / realization processes

IT/OT competency

People selection processes

Patch management

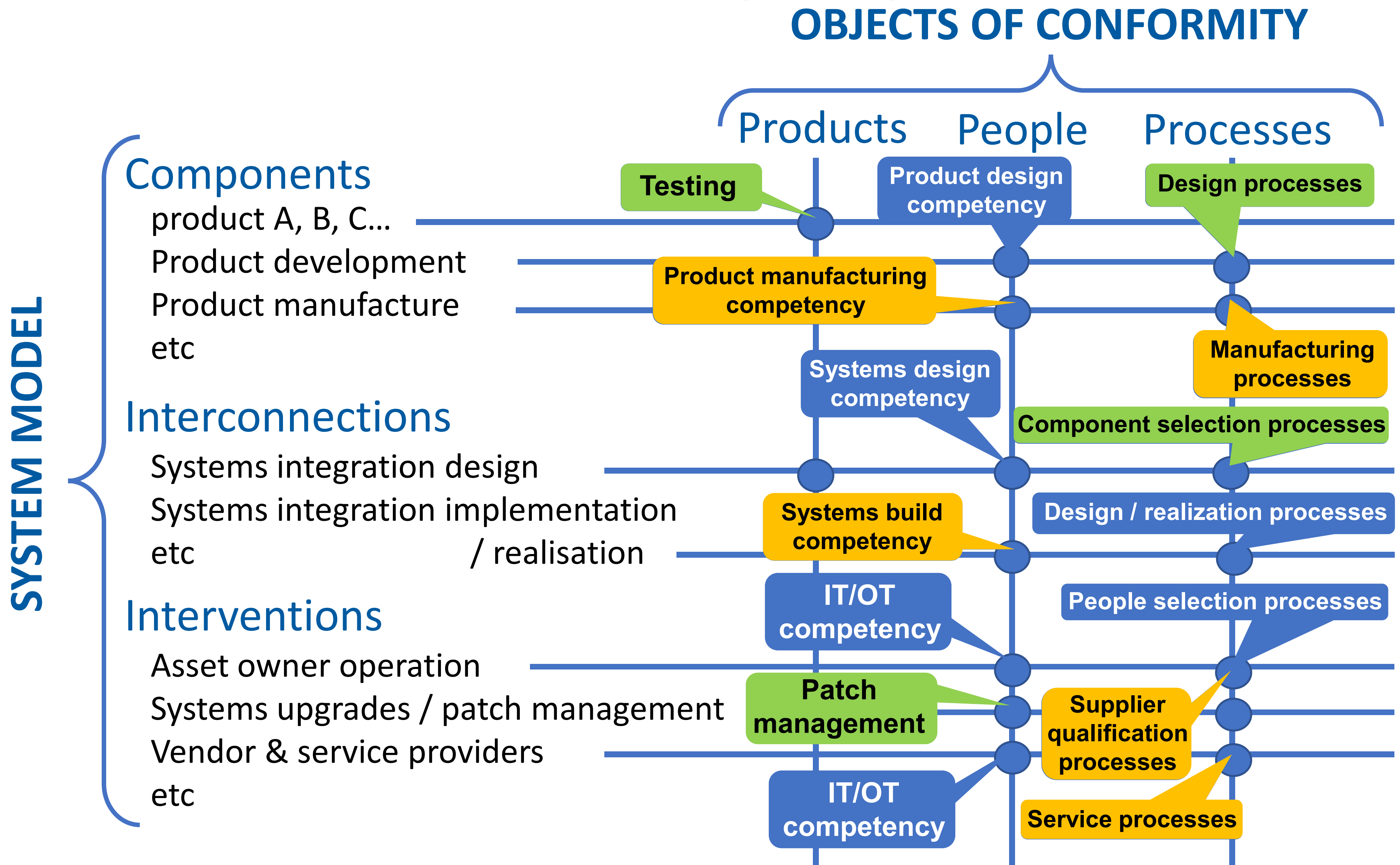
Supplier qualification processes

IT/OT competency

Service processes

Systematic Methodology

Generic Matrix Model (GMM)



OBJECTS OF CONFORMITY

Products

People

Processes

SYSTEM MODEL

Components

product A, B, C…

Product development

Product manufacture

etc

Interconnections

Systems integration design

Systems integration implementation

etc / realisation

Interventions

Asset owner operation

Systems upgrades / patch management

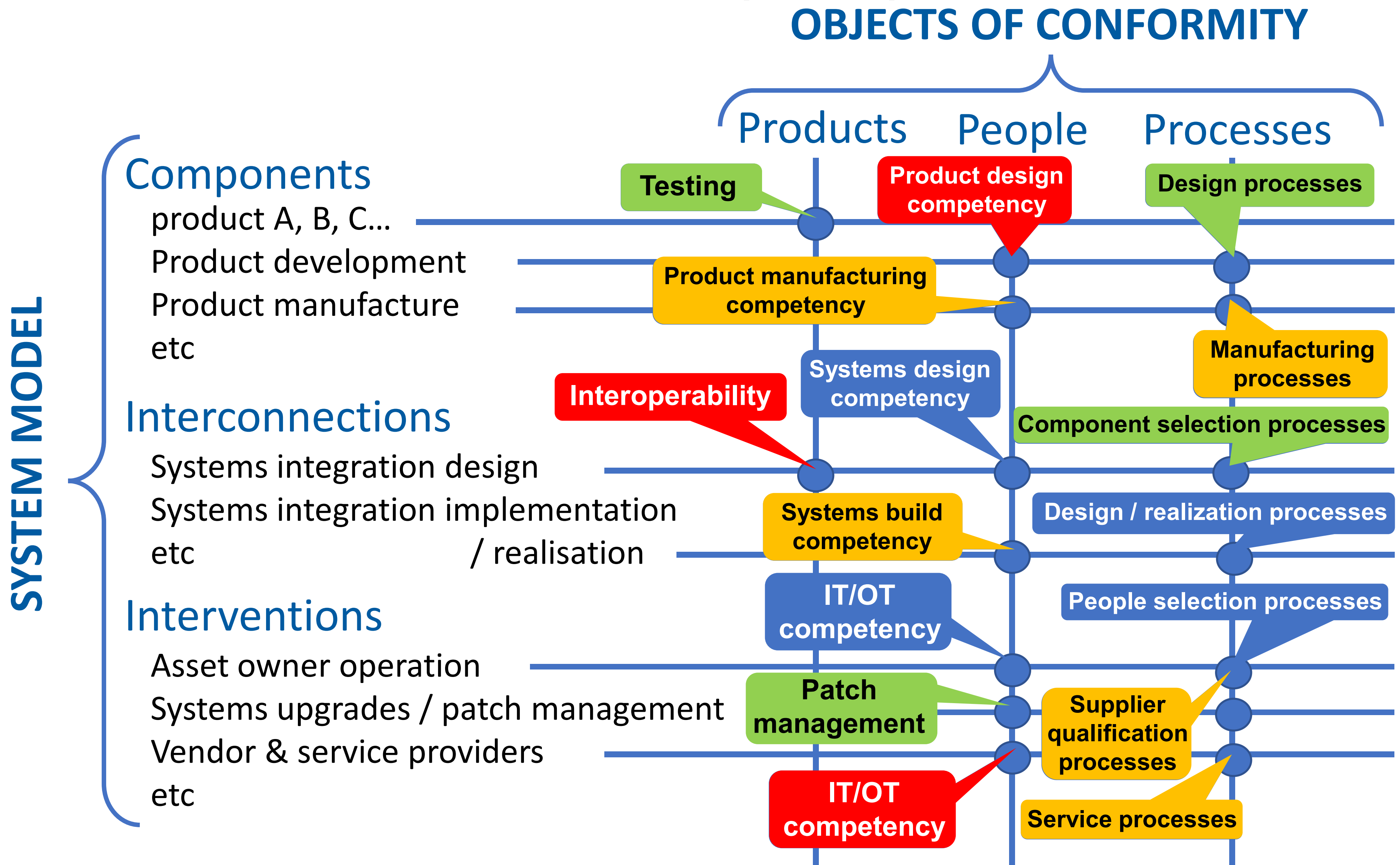
Vendor & service providers

etc

Testing
Product design competency
Design processes
Product manufacturing competency
Manufacturing processes
Systems design competency
Component selection processes
Systems build competency
Design / realization processes
IT/OT competency
People selection processes
Patch management
Supplier qualification processes
IT/OT competency
Service processes

Systematic Methodology

Generic Matrix Model (GMM)



OBJECTS OF CONFORMITY

Products People Processes

SYSTEM MODEL

Components

product A, B, C…

Product development

Product manufacture

etc

Interconnections

Systems integration design

Systems integration implementation

etc / realisation

Interventions

Asset owner operation

Systems upgrades / patch management

Vendor & service providers

etc

Testing

Product design competency

Design processes

Product manufacturing competency

Manufacturing processes

Systems design competency

Interoperability

Component selection processes

Systems build competency

Design / realization processes

IT/OT competency

People selection processes

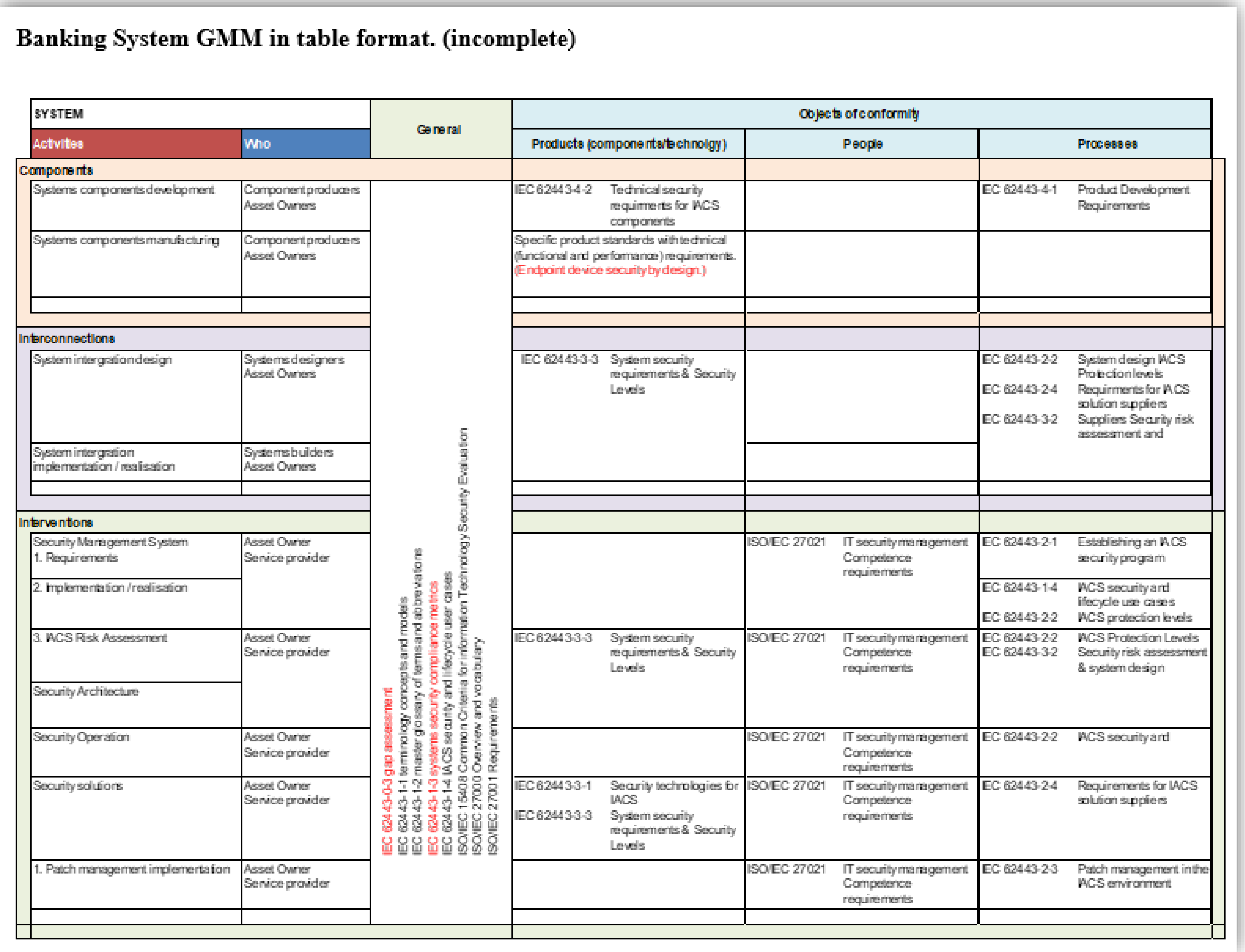
Patch management

Supplier qualification processes

IT/OT competency

Service processes

Generic Matrix Model (GMM)

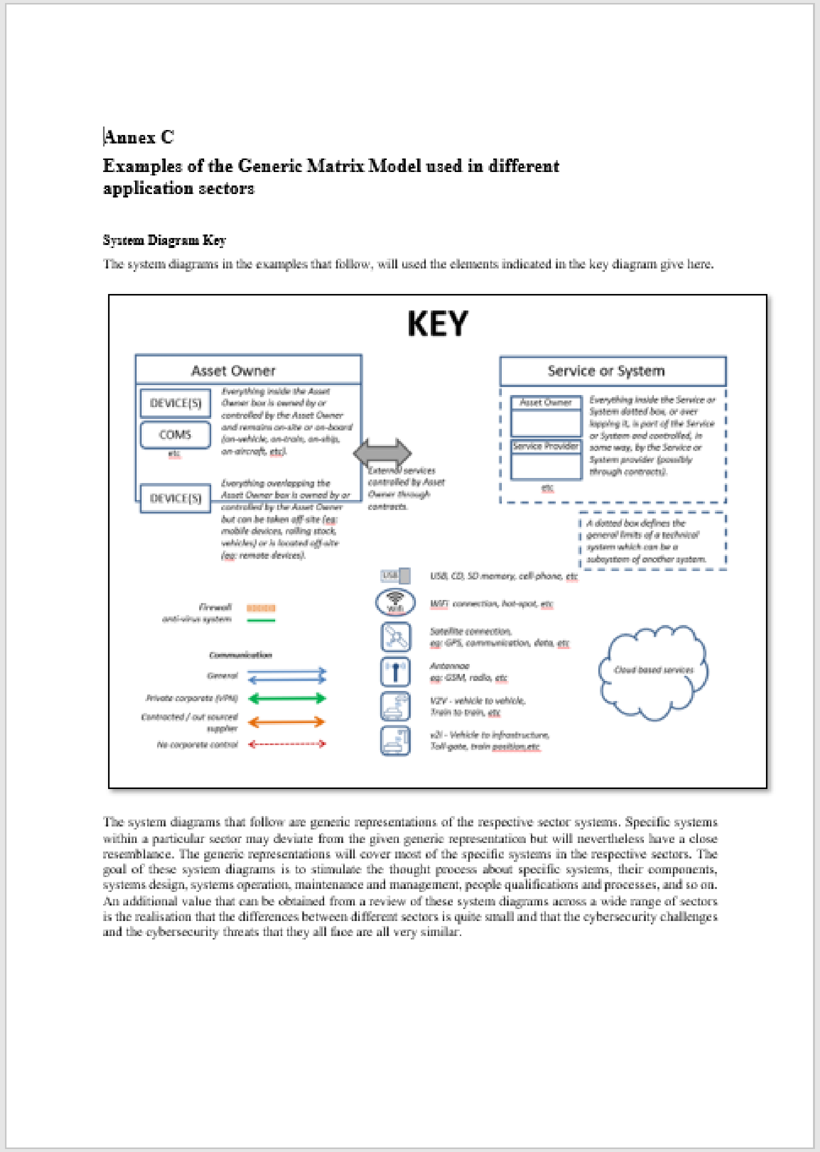


Banking System GMM in table format. (incomplete)

SYSTEM		General	Objects of conformity		
Activities	Who		Products (components/technolgy)	People	Processes
Components		IEC 62443-0-3 gap assessment IEC 62443-1-1 terminology concepts and models IEC 62443-1-2 master glossary of terms and abbreviations IEC 62443-1-3 systems security compliance metrics IEC 62443-1-4 IACS security and lifecycle user cases ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation ISO/IEC 27000 Overview and vocabulary ISO/IEC 27001 Requirements			
Systems components development	Component producers Asset Owners		IEC 62443-4-2 Technical security requirments for IACS components		IEC 62443-4-1 Product Development Requirements
Systems components manufacturing	Component producers Asset Owners		Specific product standards with technical (functional and performance) requirements. (Endpoint device security by design.)		
Interconnections					
System intergration design	Systems designers Asset Owners		IEC 62443-3-3 System security requirements & Security Levels		IEC 62443-2-2 System design IACS Protection levels IEC 62443-2-4 Requirements for IACS solution suppliers IEC 62443-3-2 Suppliers Security risk assessment and
System intergration implementation / realisation	Systems builders Asset Owners				
Interventions					
Security Management System 1. Requirements	Asset Owner Service provider			ISO/IEC 27021 IT security management Competence requirements	IEC 62443-2-1 Establishing an IACS security program
2. Implementation / realisation					IEC 62443-1-4 IACS security and lifecycle use cases IEC 62443-2-2 IACS protection levels
3. IACS Risk Assessment	Asset Owner Service provider		IEC 62443-3-3 System security requirements & Security Levels	ISO/IEC 27021 IT security management Competence requirements	IEC 62443-2-2 IACS Protection Levels IEC 62443-3-2 Security risk assessment & system design
Security Architecture					
Security Operation	Asset Owner Service provider			ISO/IEC 27021 IT security management Competence requirements	IEC 62443-2-2 IACS security and
Security solutions	Asset Owner Service provider		IEC 62443-3-1 Security technologies for IACS IEC 62443-3-3 System security requirements & Security Levels	ISO/IEC 27021 IT security management Competence requirements	IEC 62443-2-4 Requirements for IACS solution suppliers
1. Patch management implementation	Asset Owner Service provider			ISO/IEC 27021 IT security management Competence requirements	IEC 62443-2-3 Patch management in the IACS environment

Annex C - sector examples

http://www.unece.org/tradewelcome/tradewp6/groups/cybersecurity.html



Annex C

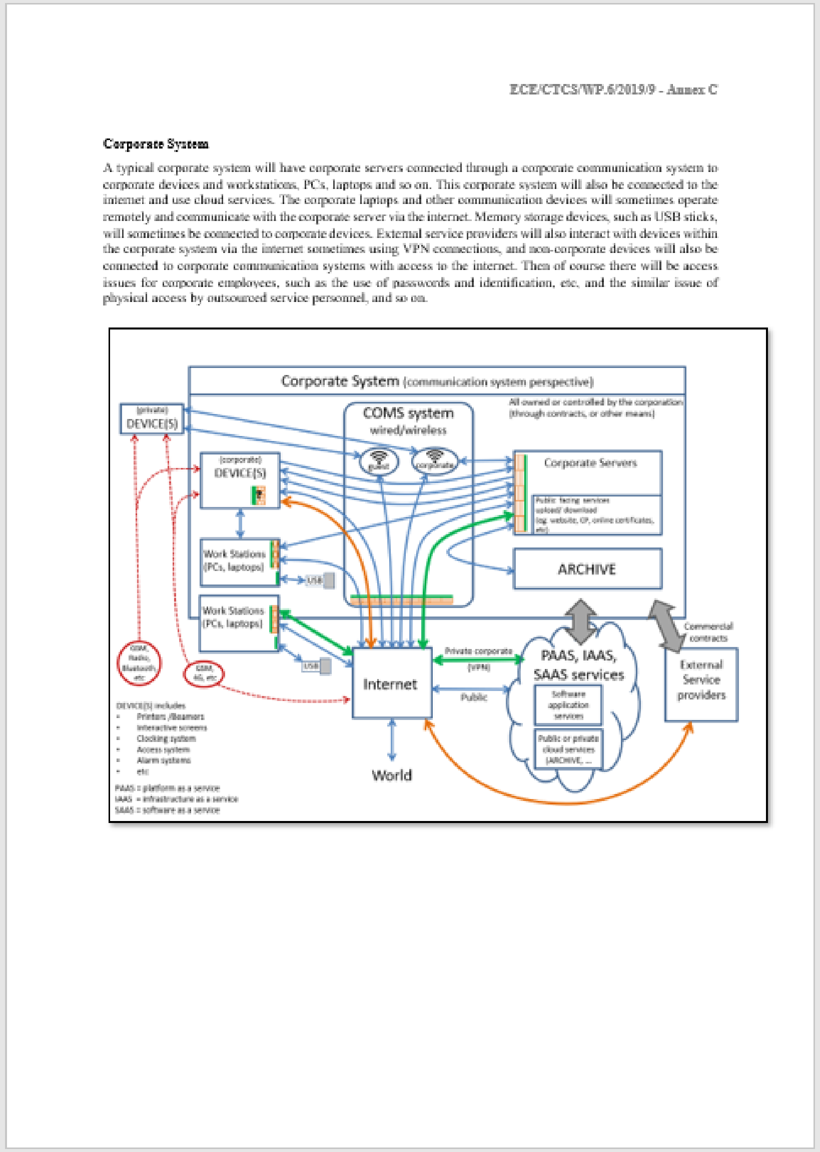
Examples of the Generic Matrix Model used in different application sectors

System Diagram Key

The system diagrams in the examples that follow, will used the elements indicated in the key diagram give here.

KEY
Asset Owner
DEVICE(S)
COMS
etc
DEVICE(S)
Everything inside the Asset Owner box is owned by or controlled by the Asset Owner and remains on-site or on-board (on-vehicle, on-train, on-ship, on-aircraft, etc).
Everything overlapping the Asset Owner box is owned by or controlled by the Asset Owner but can be taken off site (eg: mobile devices, rolling stock, vehicles) or is located off-site (eg: remote devices).
External services controlled by Asset Owner through contracts.
Service or System
Asset Owner
Service Provider
etc
Everything inside the Service or System dotted box, or over lapping it, is part of the Service or System and controlled, in some way, by the Service or System provider (possibly through contracts).
A dotted box defines the general limits of a technical system which can be a subsystem of another system.
USB
USB, CD, SD memory, cell phone, etc
Wifi
WiFi connection, hot-spot, etc
Satellite connection, eg: GPS, communication, data, etc
Antennae eg: GSM, radio, etc
V2V - vehicle to vehicle, Train to train, etc
v2i - Vehicle to infrastructure, Toll-gate, train position,etc
Firewall
anti-virus system
Communication
General
Private corporate (VPN)
Contracted / out sourced supplier
No corporate control
Cloud based services

The system diagrams that follow are generic representations of the respective sector systems. Specific systems within a particular sector may deviate from the given generic representation but will nevertheless have a close resemblance. The generic representations will cover most of the specific systems in the respective sectors. The goal of these system diagrams is to stimulate the thought process about specific systems, their components, systems design, systems operation, maintenance and management, people qualifications and processes, and so on. An additional value that can be obtained from a review of these system diagrams across a wide range of sectors is the realisation that the differences between different sectors is quite small and that the cybersecurity challenges and the cybersecurity threats that they all face are all very similar.



ECE/CTCS/WP.6/2019/9 - Annex C

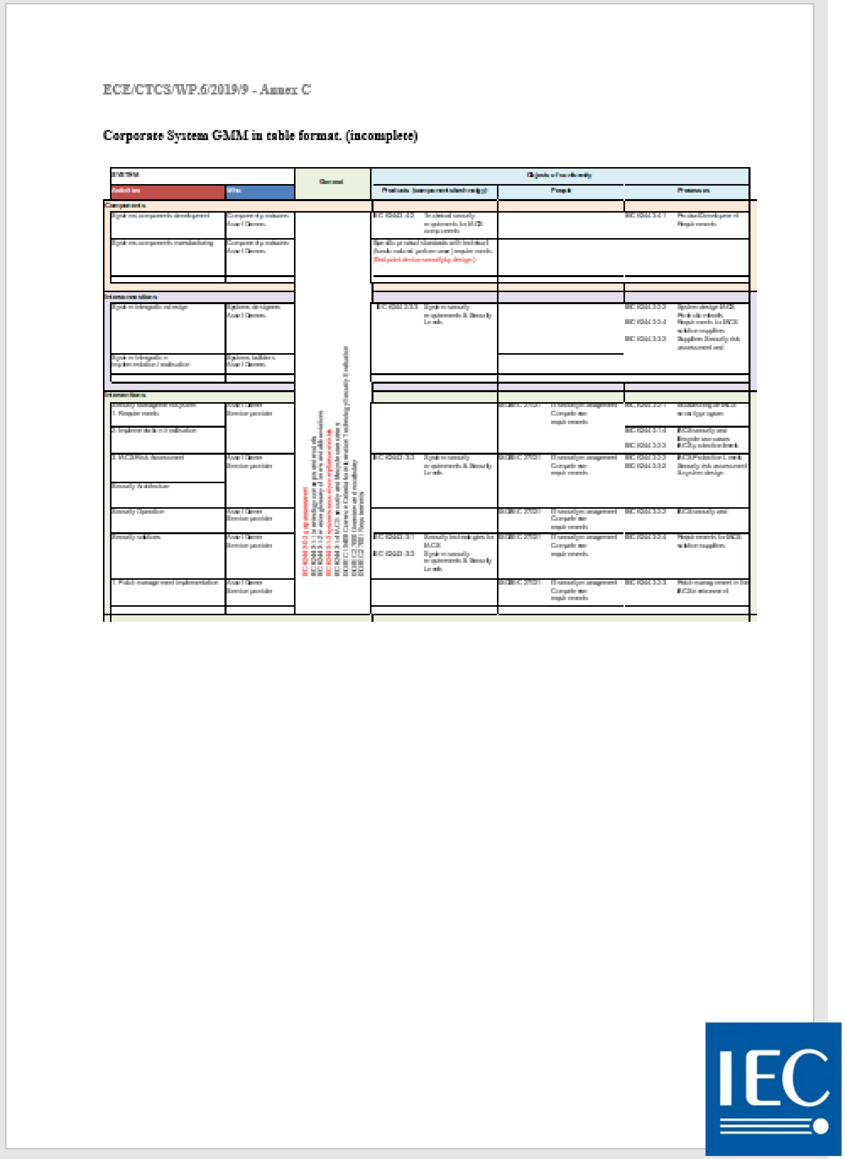
Corporate System

A typical corporate system will have corporate servers connected through a corporate communication system to corporate devices and workstations, PCs, laptops and so on. This corporate system will also be connected to the internet and use cloud services. The corporate laptops and other communication devices will sometimes operate remotely and communicate with the corporate server via the internet. Memory storage devices, such as USB sticks, will sometimes be connected to corporate devices. External service providers will also interact with devices within the corporate system via the internet sometimes using VPN connections, and non-corporate devices will also be connected to corporate communication systems with access to the internet. Then of course there will be access issues for corporate employees, such as the use of passwords and identification, etc, and the similar issue of physical access by outsourced service personnel, and so on.

Corporate System (communication system perspective)
All owned or controlled by the corporation (through contracts, or other means)
(private) DEVICE(S)
COMS system wired/wireless
guest
corporate
(corporate) DEVICE(S)
Corporate Servers
Public facing services upload/ download (eg: website, CP, online certificates, etc)
Work Stations (PCs, laptops)
USB
Work Stations (PCs, laptops)
USB
ARCHIVE
GSM, Radio, Bluetooth, etc
GSM, 4G, etc
Internet
Private corporate (VPN)
Public
PAAS, IAAS, SAAS services
Software application services
Public or private cloud services (ARCHIVE, ...
Commercial contracts
External Service providers
World

DEVICE(S) includes
- Printers /Beamers
- Interactive screens
- Clocking system
- Access system
- Alarm systems
- etc

PAAS = platform as a service
IAAS = infrastructure as a service
SAAS = software as a service

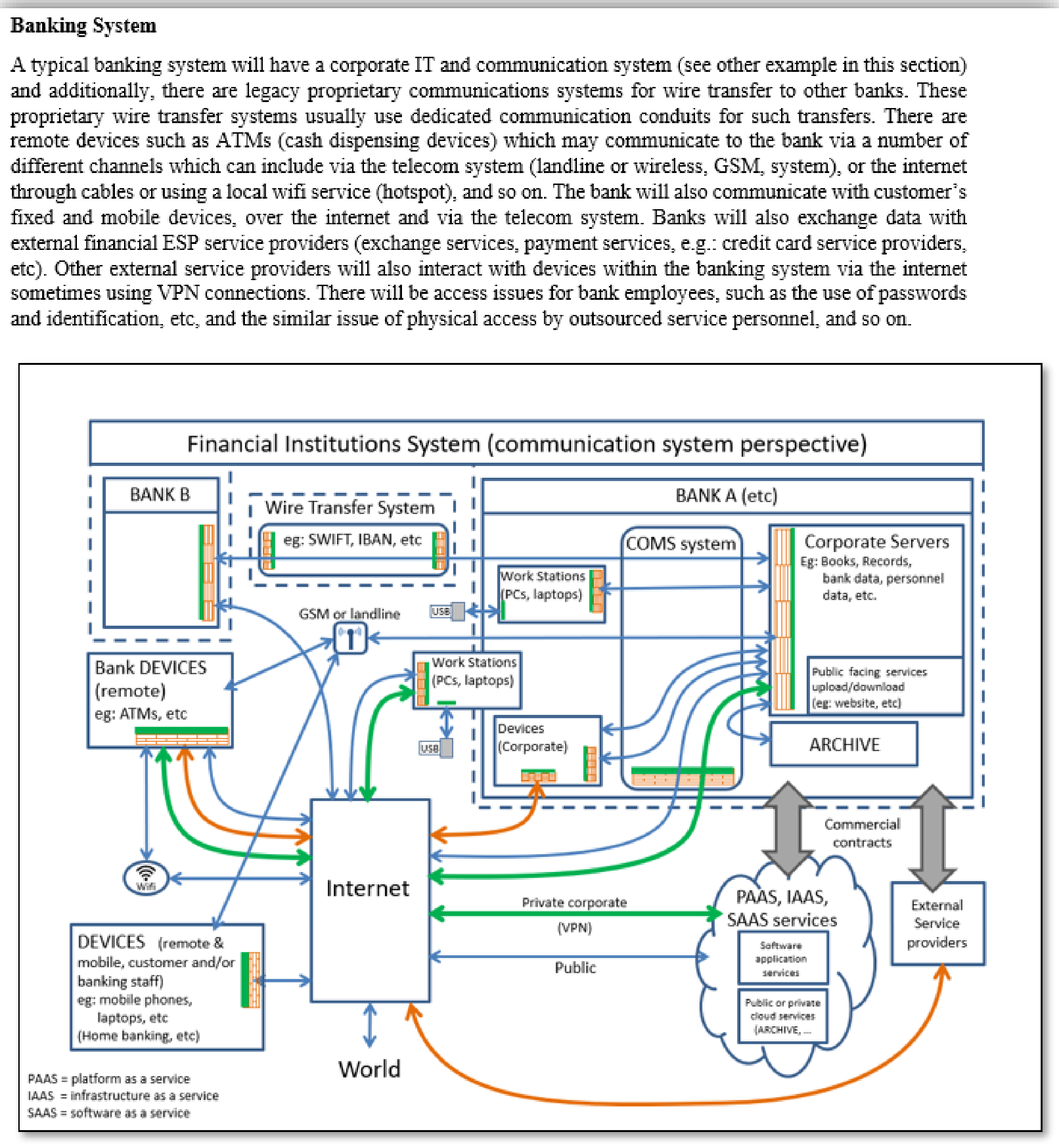


ECE/CTCS/WP.6/2019/9 - Annex C

Corporate System GMM in table format. (incomplete)

SYSTEM		General	Objects of cybersecurity		
Activities	Who		Products (component/technology)	People	Processes
Components		[illegible]			
System components development	Component suppliers Asset Owners		IEC 62443-4-2 Technical security requirements for IACS components		IEC 62443-4-1 Product Development requirements
System components manufacturing	Component suppliers Asset Owners		Specific product standards with technical (hardware and software) requirements. (End point device security by design)		
Interconnections					
System integration design	Systems designers Asset Owners		IEC 62443-3-3 System security requirements & Security Levels		IEC 62443-2-[illegible] System design IACS [illegible] IEC 62443-2-4 Requirements for IACS solution suppliers IEC 62443-[illegible] Suppliers Security risk assessment and [illegible]
System integration implementation / realisation	Systems builders Asset Owners				
Interventions					
[illegible] 1. Requirements	Asset Owners Service provider			[illegible]	[illegible]
2. Implementation / realisation					[illegible]
3. IACS Risk Assessment	Asset Owners Service provider		IEC 62443-3-3 System security requirements & Security Levels	[illegible]	[illegible]
Security Architecture					
Security Operation	Asset Owners Service provider			[illegible]	[illegible]
Security solutions	Asset Owners Service provider		IEC 62443-3-1 Security technologies for IACS IEC 62443-3-3 System security requirements & Security Levels	[illegible]	IEC 62443-2-4 Requirements for IACS solution suppliers
7. Patch management implementation	Asset Owners Service provider			[illegible]	IEC 62443-2-3 Patch management in the IACS environment

Annex C - sector examples



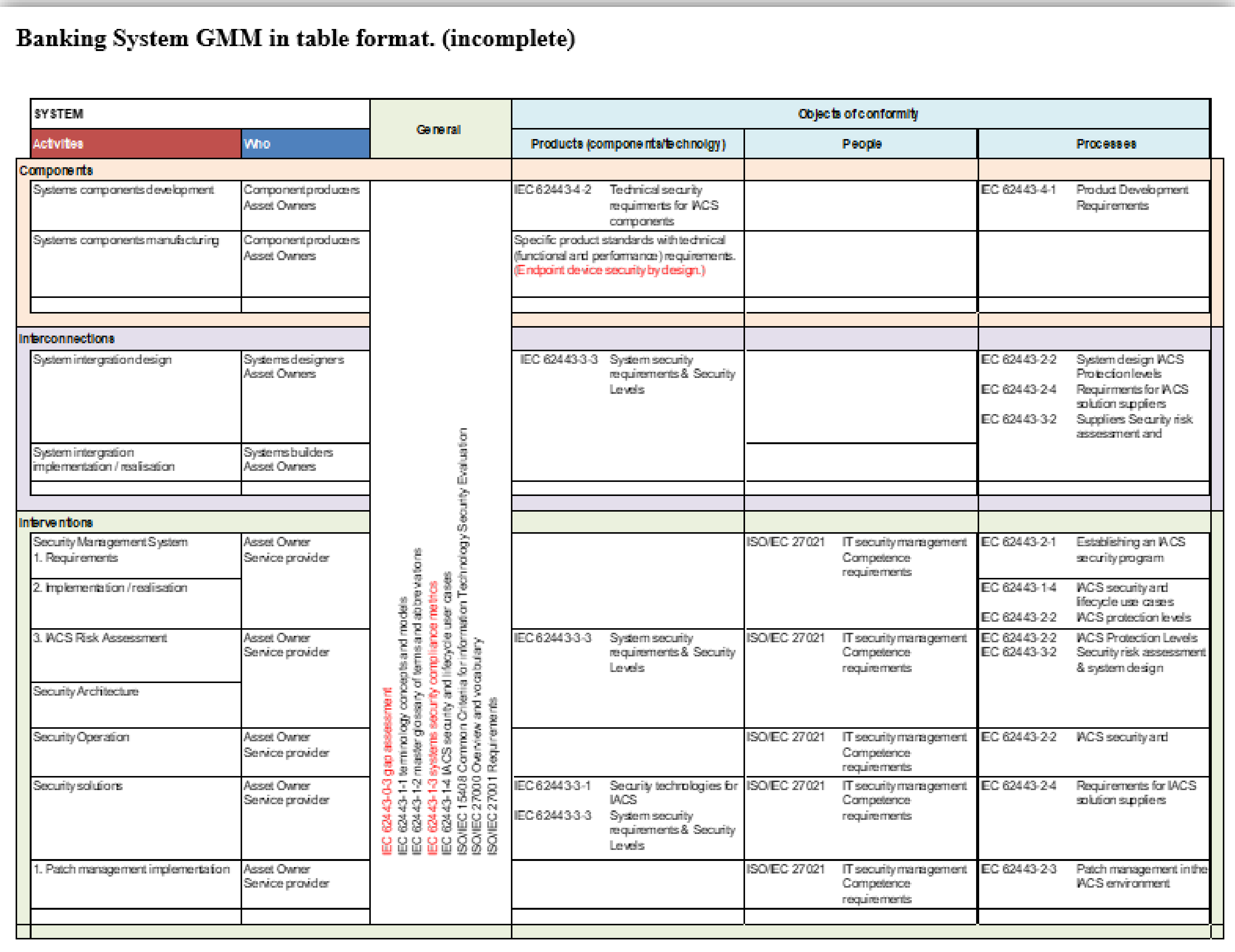
Banking System

A typical banking system will have a corporate IT and communication system (see other example in this section) and additionally, there are legacy proprietary communications systems for wire transfer to other banks. These proprietary wire transfer systems usually use dedicated communication conduits for such transfers. There are remote devices such as ATMs (cash dispensing devices) which may communicate to the bank via a number of different channels which can include via the telecom system (landline or wireless, GSM, system), or the internet through cables or using a local wifi service (hotspot), and so on. The bank will also communicate with customer's fixed and mobile devices, over the internet and via the telecom system. Banks will also exchange data with external financial ESP service providers (exchange services, payment services, e.g.: credit card service providers, etc). Other external service providers will also interact with devices within the banking system via the internet sometimes using VPN connections. There will be access issues for bank employees, such as the use of passwords and identification, etc, and the similar issue of physical access by outsourced service personnel, and so on.

Financial Institutions System (communication system perspective)
BANK B
Wire Transfer System
eg: SWIFT, IBAN, etc
BANK A (etc)
COMS system
Corporate Servers
Eg: Books, Records, bank data, personnel data, etc.
Work Stations (PCs, laptops)
USB
GSM or landline
Work Stations (PCs, laptops)
Public facing services upload/download (eg: website, etc)
Bank DEVICES (remote)
eg: ATMs, etc
USB
Devices (Corporate)
ARCHIVE
Commercial contracts
Wifi
Internet
PAAS, IAAS, SAAS services
Software application services
Public or private cloud services (ARCHIVE, ...
External Service providers
Private corporate (VPN)
Public
DEVICES (remote & mobile, customer and/or banking staff)
eg: mobile phones, laptops, etc
(Home banking, etc)
World
PAAS = platform as a service
IAAS = infrastructure as a service
SAAS = software as a service

- 8 sector examples
  - Corporate system
  - Medical network system
  - Banking system
  - Railway system
  - Traditional energy utility system
  - Smart grid electrical system
  - Active assisted living system
  - Networked vehicles

Annex C - sector examples



Banking System GMM in table format. (incomplete)

SYSTEM		General	Objects of conformity		
Activites	Who		Products (components/technolgy)	People	Processes
Components					
Systems components development	Component producers Asset Owners	IEC 62443-0-3 gap assessment IEC 62443-1-1 terminology concepts and models IEC 62443-1-2 master glossary of terms and abbreviations IEC 62443-1-3 systems security compliance metrics IEC 62443-1-4 IACS security and lifecycle user cases ISO/IEC 15408 Common Criteria for information Technology Security Evaluation ISO/IEC 27000 Overview and vocabulary ISO/IEC 27001 Requirements	IEC 62443-4-2 Technical security requirments for IACS components		IEC 62443-4-1 Product Development Requirements
Systems components manufacturing	Component producers Asset Owners		Specific product standards with technical (functional and performance) requirements. (Endpoint device security by design.)		
Interconnections					
System intergration design	Systems designers Asset Owners		IEC 62443-3-3 System security requirements & Security Levels		IEC 62443-2-2 System design IACS Protection levels IEC 62443-2-4 Requirements for IACS solution suppliers IEC 62443-3-2 Suppliers Security risk assessment and
System intergration implementation / realisation	Systems builders Asset Owners				
Interventions					
Security Management System 1. Requirements	Asset Owner Service provider			ISO/IEC 27021 IT security management Competence requirements	IEC 62443-2-1 Establishing an IACS security program
2. Implementation / realisation					IEC 62443-1-4 IACS security and lifecycle use cases IEC 62443-2-2 IACS protection levels
3. IACS Risk Assessment	Asset Owner Service provider		IEC 62443-3-3 System security requirements & Security Levels	ISO/IEC 27021 IT security management Competence requirements	IEC 62443-2-2 IACS Protection Levels IEC 62443-3-2 Security risk assessment & system design
Security Architecture					
Security Operation	Asset Owner Service provider			ISO/IEC 27021 IT security management Competence requirements	IEC 62443-2-2 IACS security and
Security solutions	Asset Owner Service provider		IEC 62443-3-1 Security technologies for IACS IEC 62443-3-3 System security requirements & Security Levels	ISO/IEC 27021 IT security management Competence requirements	IEC 62443-2-4 Requirements for IACS solution suppliers
1. Patch management implementation	Asset Owner Service provider			ISO/IEC 27021 IT security management Competence requirements	IEC 62443-2-3 Patch management in the IACS environment

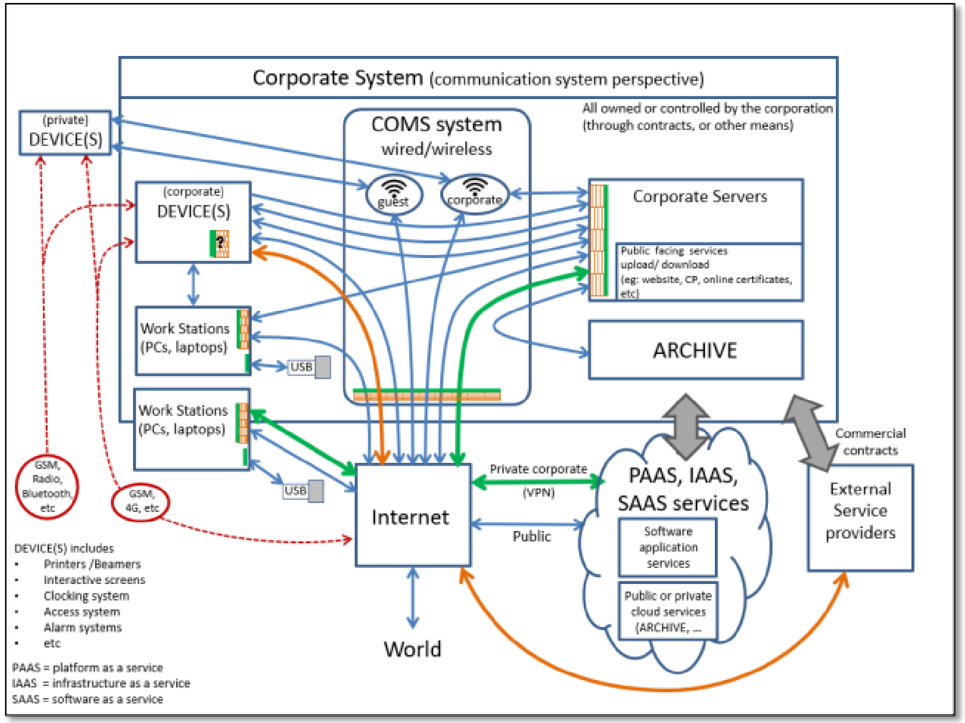
Each sector example has a GMM table indicating standards that can be used in the different phases and applications of the system.

Updating → Annex C - sector examples

ECE/CTCS/WP.6/2019/9 - Annex C

Corporate System

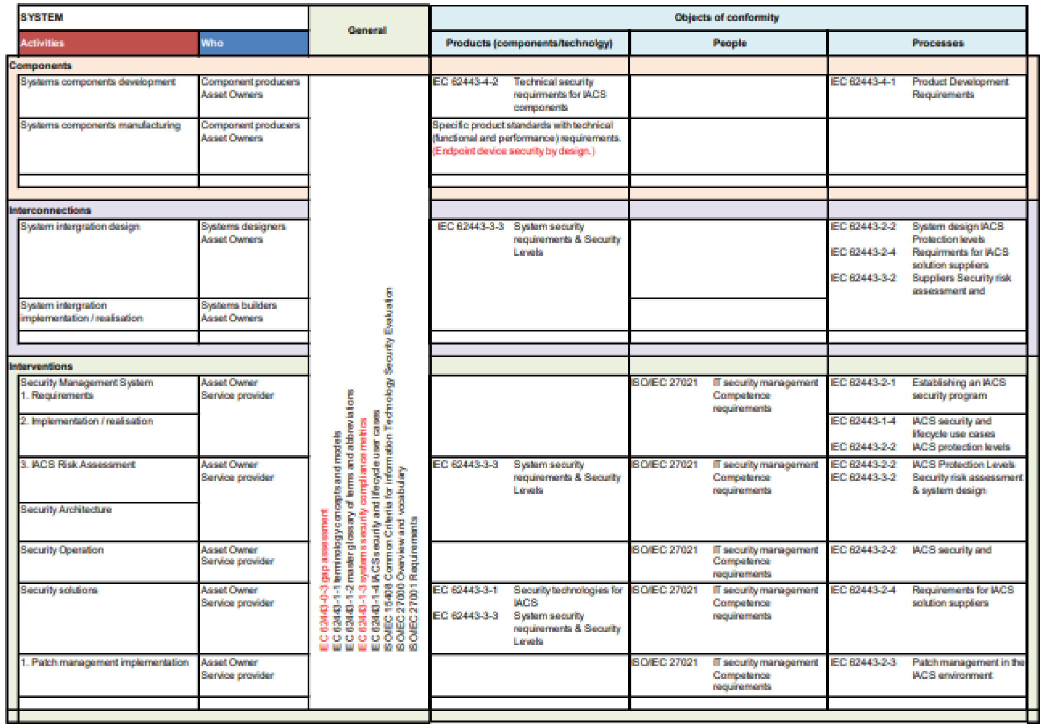
A typical corporate system will have corporate servers connected through a corporate communication system to corporate devices and workstations, PCs, laptops and so on. This corporate system will also be connected to the internet and use cloud services. The corporate laptops and other communication devices will sometimes operate remotely and communicate with the corporate server via the internet. Memory storage devices, such as USB sticks, will sometimes be connected to corporate devices. External service providers will also interact with devices within the corporate system via the internet sometimes using VPN connections, and non-corporate devices will also be connected to corporate communication systems with access to the internet. Then of course there will be access issues for corporate employees, such as the use of passwords and identification, etc, and the similar issue of physical access by outsourced service personnel, and so on.



Corporate System (communication system perspective)
All owned or controlled by the corporation (through contracts, or other means)
(private) DEVICE(S)
COMS system wired/wireless
guest
corporate
Corporate Servers
Public facing services upload/ download (eg: website, CP, online certificates, etc)
(corporate) DEVICE(S)
?
Work Stations (PCs, laptops)
USB
Work Stations (PCs, laptops)
USB
ARCHIVE
Commercial contracts
External Service providers
GSM, Radio, Bluetooth, etc
GSM, 4G, etc
Internet
Private corporate (VPN)
Public
PAAS, IAAS, SAAS services
Software application services
Public or private cloud services (ARCHIVE, ...
World
DEVICE(S) includes
• Printers /Beamers
• Interactive screens
• Clocking system
• Access system
• Alarm systems
• etc
PAAS = platform as a service
IAAS = infrastructure as a service
SAAS = software as a service

ECE/CTCS/WP.6/2019/9 - Annex C

Corporate System GMM in table format. (incomplete)



SYSTEM		General	Objects of conformity		
Activities	Who		Products (components/technolgy)	People	Processes
Components					
Systems components development	Component producers Asset Owners	IEC 62443-0-3 gap assessment IEC 62443-1-1 terminology, concepts and models IEC 62443-1-2 master glossary of terms and abbreviations IEC 62443-1-3 system security compliance metrics IEC 62443-1-4 IACS security and lifecycle use cases ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation ISO/IEC 27000 Overview and vocabulary ISO/IEC 27001 Requirements	IEC 62443-4-2 Technical security requirements for IACS components		IEC 62443-4-1 Product Development Requirements
Systems components manufacturing	Component producers Asset Owners		Specific product standards with technical (functional and performance) requirements. (Endpoint device security by design.)		
Interconnections					
System intergration design	Systems designers Asset Owners		IEC 62443-3-3 System security requirements & Security Levels		IEC 62443-2-2 System design IACS Protection levels IEC 62443-2-4 Requirments for IACS solution suppliers IEC 62443-3-2 Suppliers Security risk assessment and
System intergration implementation / realisation	Systems builders Asset Owners				
Interventions					
Security Management System 1. Requirements	Asset Owner Service provider			ISO/IEC 27021 IT security management Competence requirements	IEC 62443-2-1 Establishing an IACS security program
2. Implementation / realisation					IEC 62443-1-4 IACS security and lifecycle use cases IEC 62443-2-2 IACS protection levels
3. IACS Risk Assessment	Asset Owner Service provider		IEC 62443-3-3 System security requirements & Security Levels	ISO/IEC 27021 IT security management Competence requirements	IEC 62443-2-2 IACS Protection Levels IEC 62443-3-2 Security risk assessment & system design
Security Architecture					
Security Operation	Asset Owner Service provider			ISO/IEC 27021 IT security management Competence requirements	IEC 62443-2-2 IACS security and
Security solutions	Asset Owner Service provider		IEC 62443-3-1 Security technologies for IACS IEC 62443-3-3 System security requirements & Security Levels	ISO/IEC 27021 IT security management Competence requirements	IEC 62443-2-4 Requirements for IACS solution suppliers
1. Patch management implementation	Asset Owner Service provider			ISO/IEC 27021 IT security management Competence requirements	IEC 62443-2-3 Patch management in the IACS environment

Questions

Thank You

David Hanlon

Secretary, IEC Conformity Assessment Board (CAB)

UNECE WP.6 GRM plenary
UNOG, Geneva - remote
9th June, 2022

IEC®
International Electrotechnical Commission