# 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.



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.

#### **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 GMM in table format. (incomplete)

	SYSTEM		General	Objects of conformity					
	Activities	Who	General	Products (co	mponents/technolgy)		People		Processes
Co	Components								
	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 : (functional and pe (Endpoint device	standards with technical rformance) requirements. security by design.)				
L									
Int	arconnections								
	System intergration design	Systems designers Asset Owners		IEC 62443-3-3	System security requirements & Security Levels			EC 62443-2-2 EC 62443-2-4 EC 62443-3-2	System design IACS Protection levels Requirments for IACS solution suppliers Suppliers Security risk
-	System intergration implementation / realisation	Systems builders Asset Owners	/ Evaluation						assessment and
			f						
Int	erventions		Sec						
ſ	Security Management System 1. Requirements	Asset Owner Service provider	tions inology (			ISO/IEC 27021	IT security management Competence requirements	IEC 62443-2-1	Establishing an IACS security program
	2. Implementation / realisation		odels abbrevia metrics ser cases ation Tech					IEC 62443-1-4 IEC 62443-2-2	IACS security and lifecycle use cases IACS protection levels
	3. IACS Risk Assessment	Asset Owner Service provider	spts and me f terms and ompliance lifecycle u for informs cabulary	IEC 62443-3-3	System security requirements & Security Levels	ISO/IEC 27021	IT security management Competence requirements	IEC 62443-2-2 IEC 62443-3-2	IACS Protection Levels Security risk assessment & system design
	Security Architecture		ssment gy conce ossary o ssary o ecurity and urity and Criteria and voc						
	Security Operation	Asset Owner Service provider	gap asses terminolog systems s IACS sec Common Overview Requirem			ISO/IEC 27021	IT security management Competence requirements	IEC 62443-2-2	IACS security and
	Security solutions	Asset Owner Service provider	IEC 62443-0-3 IEC 62443-1-1 EC 62443-1-2 IEC 62443-1-3 IEC 62443-1-3 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 627000 IEC 27000	IEC 62443-3-1 IEC 62443-3-3	Security technologies for IACS 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
-			l					I	

#### **Medical Network System**

A typical medical network system will have a corporate IT and communication system (see other example in this section), additionally there will be other proprietary communication systems to specific medical devices. These proprietary systems will use dedicated communication conduits for control and monitoring of devices. There will be other devices controlled and monitored over a common IT communication system. Data will be exchanged with external entities such as other hospitals, doctors, pharmacies, families, medical research organizations, etc. External service providers will also interact with devices within the medical network system via the internet sometimes using VPN connections. There will be access issues for medical network employees, such as the use of passwords and identification, etc, and the similar issue of physical access by outsourced service personnel, and so on.



#### Medical Network System GMM in table format. (incomplete)

SYSTEM					Object	s of conformity		
Activities	Who	General	Products (co	mponents/technolgy)		People		Processes
Components								
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 (functional and pe (Endpoint device	standards with technical erformance) requirements. security by design.)				
Interconnections	1-							
System intergration design	Systems designers Asset Owners		IEC 62443-3-3	System security requirements & Security			EC 62443-2-2	System design IACS Protection levels
				201013			EC 62443-3-2	solution suppliers
		5					20 02 110 0 2	assessment and
System intergration implementation / realisation	Systems builders Asset Owners	aluati						
		́ш,						
	-	nrif.						
Interventions		Sec						
Security Management System 1. Requirements	Asset Owner Service provider	ions nology			ISO/IEC 27021	IT security management Competence	IEC 62443-2-1	Establishing an IACS security program
2. Implementation / realisation		els obreviat etrics r cases on Tech				requirements	IEC 62443-1-4	IACS security and lifecycle use cases
		d at e m use					IEC 62443-2-2	IACS protection levels
3. IACS Risk Assessment	Asset Owner Service provider	spts and rr f terms an complianc briffecycle i for inform cabulary	IEC 62443-3-3	System security requirements & Security Levels	ISO/IEC 27021	IT security management Competence requirements	IEC 62443-2-2 IEC 62443-3-2	ACS Protection Levels Security risk assessment & system design
Security Architecture		ssment gy conce ossary o ecurity and urity and Criteria and voi						
Security Operation	Asset Owner Service provider	Jap asses erminoloç naster glc systems s ACS se cr Commo n Overview Requirem			ISO/IEC 27021	IT security management Competence requirements	IEC 62443-2-2	IACS security and
Security solutions	Asset Owner	0008 4	IEC 62443-3-1	Security technologies for	ISO/IEC 27021	IT security management	IEC 62443-2-4	Requirements for IACS
	Service provider	IEC 62443-0 IEC 62443-1 IEC 62443-1 IEC 62443-1 IEC 62443-1 IEC 62443-1 IEC 62443-1 IEC 62443-1 IEC 62443-1 IEC 62443-1 IEC 6220 ISO/IEC 270 ISO/IEC 270	IEC 62443-3-3	ACS System security requirements & Security Levels		Competence requirements		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

Other standards:

- IEC 80001-5-1 Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software --- Part 5: Security Part 5-1: Activities in the product lifecycle
- IEC 60601-4-5 Medical Equipment --- Part 4-5: Guidance and interpretation Safety related technical security specifications for medical devices → mapped to IEC 62443-4-2
- IEC 80001 Application of risk management for IT-networks incorporating medical devices –Part 1: Roles, responsibilities and activities
- IEC 80001-2-2 Communicating Security Needs, Risks & Controls (19 Capabilities)
- IEC 80001-2-3 Wireless Guidance
- IEC 80001-2-4 HDO Implementation Guidance
- IEC 80001-2-5 Distributed Alarm Systems
- IEC 80001-2-6 Responsibility Agreements
- IEC 80001-2-7 Conformance Self-assessment Guidance
- IEC 80001-2-8 Mapping Security Controls to the 19 Capabilities of IEC 80001-2-2, NIST 853, ISO/IEC 15408-2 (CC), ISO/IEC 15408-3, IEC 62443-3-3, ISO/IEC 27002.
- IEC 80001-2-9 Security Assurance Case for the 19 Capabilities of IEC 80001-2-2
- IEC 62304 medical device lifecycle standards ← nothing on cybersecurity
- IEC 82304 health software ← small amount on cybersecurity
- ISO 14971 application of risk management to medical devices (mostly safety issues)

#### **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.



## Banking System GMM in table format. (incomplete)

	SYSTEM		General	Objects of conformity					
	Activities	Who	General	Products (co	mponents/technolgy)		People		Processes
Co	Components								
	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 : (functional and pe (Endpoint device	standards with technical rformance) requirements. security by design.)				
L									
Int	arconnections								
	System intergration design	Systems designers Asset Owners		IEC 62443-3-3	System security requirements & Security Levels			EC 62443-2-2 EC 62443-2-4 EC 62443-3-2	System design IACS Protection levels Requirments for IACS solution suppliers Suppliers Security risk
-	System intergration implementation / realisation	Systems builders Asset Owners	/ Evaluation						assessment and
			f						
Int	erventions		Sec						
ſ	Security Management System 1. Requirements	Asset Owner Service provider	tions inology (			ISO/IEC 27021	IT security management Competence requirements	IEC 62443-2-1	Establishing an IACS security program
	2. Implementation / realisation		odels abbrevia metrics ser cases ation Tech					IEC 62443-1-4 IEC 62443-2-2	IACS security and lifecycle use cases IACS protection levels
	3. IACS Risk Assessment	Asset Owner Service provider	spts and me f terms and ompliance lifecycle u for informs cabulary	IEC 62443-3-3	System security requirements & Security Levels	ISO/IEC 27021	IT security management Competence requirements	IEC 62443-2-2 IEC 62443-3-2	IACS Protection Levels Security risk assessment & system design
	Security Architecture		ssment gy conce ossary o ssary o ecurity and urity and Criteria and voc						
	Security Operation	Asset Owner Service provider	gap asses terminolog systems s IACS sec Common Overview Requirem			ISO/IEC 27021	IT security management Competence requirements	IEC 62443-2-2	IACS security and
	Security solutions	Asset Owner Service provider	IEC 62443-0-3 IEC 62443-1-1 EC 62443-1-2 IEC 62443-1-3 IEC 62443-1-3 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 627000 IEC 27000	IEC 62443-3-1 IEC 62443-3-3	Security technologies for IACS 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
-			l					I	

#### **Railway System**

The railway example was developed on the basis of the European rail system with rollingstock transiting across multiple countries with control responsibility being handed between multiple control centres, energy management centres, signalling centres and so on. A typical railway system has a lot of non-connected legacy infrastructure and a lot of new connected infrastructure with a strong trend towards the latter. A typical railway system has five subsystems being the rolling stock itself, fixed infrastructure such as the tracks, switchgear, overhead lines, railway stations, night depots, etc, an energy control, measurement and billing system, a signalling system and an operations and traffic control management system (ERTMS in Europe). There is much communication between these systems over dedicated proprietary communications systems, over telecom systems, over radio systems, over satellite system, of wifi and internet systems, and so on. There is also train to train communication, train to fixed infrastructure communication and train to controller communication, and so on. There are external service providers and many railways employees with their respective access rights and identification issues. Control of the rail system is divided into cells with lengths of track divide in virtual blocks.



## Railway System GMM in table format. (incomplete)

3	SYSTEM		0	Objects of conformity					
A	ctivities	Who	General	Products (co	mponents/technolgy)		People		Processes
Con	Components								
S	ystems components development	Component producers Asset Owners		IEC 62443-4-2	Technical security requirments for IACS components			IEC 62443-4-1	Product Development Requirements
S	ystems components manufacturing	Component producers Asset Owners		Specific product (functional and pe (Endpoint device	standards with technical rformance) requirements. security by design.)				
Inte	rconnections								
S	ystem intergration design	Systems designers Asset Owners		IEC 62443-3-3	System security requirements & Security Levels			IEC 62443-2-2 IEC 62443-2-4	System design IACS Protection levels Requirments for IACS solution suppliers
			tion					IEC 62443-3-2	Suppliers Security risk assessment and
S	ystem intergration nplementation / realisation	Systems builders Asset Owners	Evalua						
			lity						
			so nu						
Inte	rventions		Se						
S 1.	ecurity Management System . Requirements	Asset Owner Service provider	tions *			ISO/IEC 27021	IT security management Competence requirements	IEC 62443-2-1	Establishing an IACS security program
2.	Implementation / realisation		dels abbrevia metrics ser casee tion Tecl				·	IEC 62443-1-4 IEC 62443-2-2	IACS security and lifecycle use cases IACS protection levels
3.	IACS Risk Assessment	Asset Owner Service provider	ots and mc terms and ompliance lifecycle u for informa abulary	IEC 62443-3-3	System security requirements & Security Levels	ISO/IEC 27021	IT security management Competence requirements	IEC 62443-2-2 IEC 62443-3-2	ACS Protection Levels Security risk assessment & system design
S	ecurity Architecture		ssment gy concel ossary of security α urity and 'Criterila ' and voc: nents						
S	ecurity Operation	Asset Owner Service provider	gap asse: terminolo master gla systems s MCS sec Common Overview Requiren			ISO/IEC 27021	IT security management Competence requirements	IEC 62443-2-2	IACS security and
S	ecurity solutions	Asset Owner Service provider	IEC 62443-0-3 IEC 62443-1-1 IEC 62443-1-2 IEC 62443-1-3 IEC 62443-1-3 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 627001 IEC 6270001 IEC 627001 IEC 6270001 IEC 627000000000000000000000000000000000000	IEC 62443-3-1 IEC 62443-3-3	Security technologies for IACS 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
		I							

#### **Traditional Energy Utility System**

Traditionally an Energy Utility System is a centralised system with a generation system, transmission system and a distribution system. There will be a corporate IT system (see other example in this section) but additionally there will be industrial control systems. These industrial control systems will traditionally use corporate industrial communication conduits for control and monitoring of devices on the different generation, transmission and distribution systems. Some devices will also be controlled and monitored over a common IT communication system. Currently, there is a trend towards the use of public communication systems to monitor and control some remote devices. This trend is being driven by economic factors. Remote devices in the future will therefore be more and more so controlled and monitored using communication over the internet and then to the corporate industrial system and/or the corporate IT system. 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. 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.



## Traditional Energy Utility System GMM in table format. (incomplete)

SYSTEM					Object	s of conformity		
Activities	Who	General	Products (co	mponents/technolgy)		People	1	Processes
Components								
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 (functional and pe (Endpoint device	standards with technical erformance) requirements. security by design.)				
Interconnections								
Sustem intergration design	Suntama dagignora		IEC 63443 3 3	Sustem accurity			IEC 63443 3 3	Suntom design IACS
System mergration design	Asset Owners		IEC 02440-0-0	requirements & Security Levels			IEC 62443-2-2	Protection levels Requirments for IACS
		- ug					IEC 62443-3-2	Suppliers Security risk assessment and
System intergration implementation / realisation	Systems builders Asset Owners	Evaluat						
		₹						
Interventions		ecr						
Security Management System 1. Requirements	Asset Owner Service provider	tions nology S			ISO/IEC 27021	IT security management Competence	IEC 62443-2-1	Establishing an IACS security program
2. Implementation / realisation		dels abbrevia metrics ser cases trion Tech				requirementa	IEC 62443-1-4 IEC 62443-2-2	ACS security and lifecycle use cases IACS protection levels
3. IACS Risk Assessment	Asset Owner Service provider	ots and me terms and mpliance lifecycle u for informa abulary	IEC 62443-3-3	System security requirements & Security Levels	ISO/IEC 27021	IT security management Competence requirements	IEC 62443-2-2 IEC 62443-3-2	ACS Protection Levels Security risk assessment & system design
Security Architecture		ssment gy concep ossary of i ecurity co urity and l Criteriia f and voca						
Security Operation	Asset Owner Service provider	Jap asses erminoloç master glc systems s ACS sec Common Overview Requirem			ISO/IEC 27021	IT security management Competence requirements	IEC 62443-2-2	IACS security and
Security solutions	Asset Owner Service provider	EC 62443-0-3 EC 62443-1-1 EC 62443-1-1 EC 62443-1-3 EC 62443-1-3 EC 62443-1-4 EC 62443-1-4 EC 62443-1-4 EC 62443-1-4 I SO/IEC 27000 I SO/IEC 27001	IEC 62443-3-1 IEC 62443-3-3	Security technologies for IACS 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
		l			l			

#### **Smart Grid Electrical System**

The smart grid electrical system is different from a traditional electrical utility system in that there is no centralized electrical energy generation, and no transmission system. However, there is a distribution system which is a bidirectional system where energy can flow in all directions. There are many energy producers on the system who in most cases are also energy consumers (prosumers). For example, homeowners or companies with PV panels will, at certain times, produce energy and inject it onto the distribution grid, and, at other times, feed energy off the grid. A traditional electrical utility may also be a supplier to the grid. Each prosumer will have a smart meter to measure the flow of energy in either direction and communicate correct billing. This system will not have a single asset owner, but rather each energy producer will be a part owner of the system. The management of energy flow will be distributed and imbedded in devices on the system. External service providers will provide patch management and other services. Much of the communication will occur over telecom and internet systems.



## Smart Grid Electrical System GMM in table format. (incomplete)

SYSTEM		General			Objects of conformity				
Activities	Who	General	Products (co	mponents/technolgy)		People		Processes	
Components									
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 (functional and pe (Endpoint device	standards with technical erformance) requirements. security by design.)					
Interconnections									
Puptom intergration design	Sustama dagignom		IEC 63443 3 3	Suptom acquisity			EC 62442.2.2	Sustem design IACS	
System mergration design	Asset Owners		IEC 02443-3-3	requirements & Security			EC 02443-2-2	Protection levels	
				Levels			IEC 62443-2-4	Requirments for IACS	
		5					IEC 62443-3-2	Suppliers Security risk assessment and	
System intergration	Systems builders	uati							
Implementation / realisation	Asset Owners	Eval							
		È							
Interventions		ecn							
Security Management System	Asset Owner	S ≥			ISO/IEC 27021	IT security management	IEC 62443-2-1	Establishing an IACS	
1. Requirements	Service provider	ions nolog			00/120 27021	Competence	20 02440-2-1	security program	
2. Implementation / realisation	1	wiat ses ech				requirements	IEC 62443-1-4	IACS security and	
		bbre bbre sr ca						lifecycle use cases	
		nation nation		-			EC 62443-2-2	IACS protection levels	
3. IACS Risk Assessment	Asset Owner Service provider	and r ms ar plianc cycle cycle inforr inforr	IEC 62443-3-3	System security requirements & Security	ISO/IEC 27021	IT security management Competence	IEC 62443-2-2 IEC 62443-3-2	IACS Protection Levels Security risk assessment	
		a for cabu		Levels		requirements		& system design	
Security Architecture		sment by cono sssary c ssary c ecurity and cutterii and vo ients							
Security Operation	Asset Owner	sses riglo secu non riew			ISO/IEC 27021	IT security management	IEC 62443-2-2	IACS security and	
	Service provider	Jap a: ermin aster ACS Comr Comr Requ				Competence requirements			
Security solutions	Asset Owner	00087 <mark>-2</mark> -2-7	IEC 62443-3-1	Security technologies for	ISO/IEC 27021	IT security management	IEC 62443-2-4	Requirements for IACS	
	Service provider	IEC 62443- EEC 62443- EEC 62443- IEC 62443- IEC 62443- IEC 62443- IEC 62443- IEC 62443- IEC 62443- IEC 62443- IEC 6220 IEC 6220 IEC 6270 IEC 62700 IEC 62700 IEC 6270 IEC 6270 IEC 62700 IEC 62700 IEC 62	IEC 62443-3-3	IACS System security requirements & Security Levels		Competence requirements		solution suppliers	
1. Patch management implementation	Asset Owner				ISO/IEC 27021	IT security management	IEC 62443-2-3	Patch management in the	
	Service provider					Competence requirements		IACS environment	

#### Active Assisted Living (AAL) System

Future AAL, or active assisted living systems, for the elderly, will use home devices and wearables to monitor and communicate health and activity data to an AAL service provider. The AAL service providers will receive data and transform that into information which will be communicated to health services such as a doctor or hospital, which may then prescribe medications and thus communicate with a pharmacy, and so on. And of course, information may be communicated to family members, and so on. External service providers will also ensure the correct functioning of the remote devices used by the elderly, provide remote updates and patch management, and so on.



#### SYSTEM Objects of conformity General Activities Nho Products (components/technolgy) People Processes Components Technical security requirments for IACS components Systems components development Component producers Asset Owners IEC 62443-4-2 EC 62443-4-1 Product Development Requirements Component producers Asset Owners Specific product standards with technical (functional and performance) requirements (Endpoint device security by design.) Systems components manufacturing Interconnections System intergration design IEC 62443-3-3 System security requirements & Security EC 62443-2-2 System design IACS Systems designers Asset Owners Protection lev Requirments for IACS solution suppliers Suppliers Security risk Levels IEC 62443-2-4 EC 62443-3-2 EC 62443-0-3 gap assessment EC 62443-1-1 Errimology or companies and abbreviations EC 62443-1-1 Errimology or companies methods EC 62443-12 Stater glossary of terms and abbreviations EC 62443-13 Stater security and theoryte user cases State 1-1 ALCS security and theoryte user cases State 27400 R Common Criteria for information Technology Security Evaluation State 27400 R Requirements State 27401 R equirements assessment and System intergration implementation / realisation Systems builders Asset Owners nterventions Security Management System 1. Requirements ISO/IEC 27021 Establishing an IACS security program Asset Owner IT security management IEC 62443-2-1 Competence requirements Service provider 2 Implementation / realisation EC 62443-1-4 IACS security and lifecycle use cases IACS protection levels EC 62443-2-2 3. IACS Risk Assessment Asset Owner Service provider IEC 62443-3-3 System security requirements & Security ISO/IEC 27021 IT security manage IEC 62443-2-2 IEC 62443-3-2 IACS Protection Levels Security risk assessmen Competence requirements Levels & system design Security Architecture ISO/IEC 27021 Security Operation Asset Owner IT security manage IEC 62443-2-2 IACS security and nt Service provider Competence requirements Security technologies for IACS System security requirements & Security Levels Requirements for IACS solution suppliers Asset Owner Service provider ecurity solutions IEC 62443-3-1 ISO/IEC 27021 IT security management Competence EC 62443-2-4 IEC 62443-3-3 requirements IT security manage Competence requirements Asset Owner Service provider Patch management in the IACS environment 1. Patch management implementatio ISO/IEC 27021 IEC 62443-2-3

### Active Assisted Living (AAL) System GMM in table format. (incomplete)

#### **Networked Vehicles System**

Networked vehicles is a current and future application. In this case the device, a vehicle, is mobile and can of course be very dangerous for those being transported and/or for those nearby. In this case data is transmitted over various communication channels and can be unidirectional, or bidirectional. The data may simply be entertainment information or could be GPS and other position or traffic information, or could be vehicle performance data, or could be vehicle to vehicle detection and communication, or vehicle to infrastructure communication (toll gates, toll tunnels, toll bridges, etc) or could be vehicle-systems upgrade information, and so on.



## Networked Vehicles System GMM in table format. (incomplete)

SYSTEM				Objects of conformity						
Activities	Who	General	Products (co	mponents/technolgy)		People		Processes		
Components	Components									
Systems components development	t Component producers Asset Owners		IEC 62443-4-2	Technical security requirments for IACS components			IEC 62443-4-1	Product Development Requirements		
Systems components manufacturin	g Component producers Asset Owners		Specific product : (functional and pe (Endpoint device	standards with technical erformance) requirements. security by design.)						
Interconnections										
System intergration design	Systems designers Asset Owners		IEC 62443-3-3	System security requirements & Security Levels			IEC 62443-2-2 IEC 62443-2-4	System design IACS Protection levels Requirments for IACS solution suppliers		
		tion					IEC 62443-3-2	Suppliers Security risk assessment and		
System intergration implementation / realisation	Systems builders Asset Owners	Evalua								
		rity								
Interventions		ecu								
Security Management System 1. Requirements	Asset Owner Service provider	tions inology S			ISO/IEC 27021	IT security management Competence	IEC 62443-2-1	Establishing an IACS security program		
2. Implementation / realisation		odels abbrevia metrics ser cases ation Tech				roquironiono	IEC 62443-1-4 IEC 62443-2-2	ACS security and lifecycle use cases IACS protection levels		
3. IACS Risk Assessment	Asset Owner Service provider	pts and mo terms and ompliance lifecycle u for informs abulary	IEC 62443-3-3	System security requirements & Security Levels	ISO/IEC 27021	IT security management Competence requirements	IEC 62443-2-2 IEC 62443-3-2	IACS Protection Levels Security risk assessment & system design		
Security Architecture		ssment gy conce ossary of ecurity of urity and Urity and Criteria and voc								
Security Operation	Asset Owner Service provider	gap assee terminolog master glo systems s IACS sec Common Overview Requirem			ISO/IEC 27021	IT security management Competence requirements	IEC 62443-2-2	IACS security and		
Security solutions	Asset Owner Service provider	IEC 62443-0-3 IEC 62443-1-1 IEC 62443-1-2 IEC 62443-1-3 IEC 62443-1-3 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 62443-1-4 IEC 627001 IEC 6270000 IEC 6270000 IEC 6270000 IEC 6270000 IEC 6270000 IEC 6270000 IEC 6270000 IEC 6270000 IEC 627000000000000000000000000000000000000	IEC 62443-3-1 IEC 62443-3-3	Security technologies for IACS 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 implementat	ion Asset Owner Service provider				ISO/IEC 27021	IT security management Competence requirements	IEC 62443-2-3	Patch management in the IACS environment		