United Nations ECE/CTCS/WP.6/2018/9

Economic and Social Council

Distr.: General
10 September 2018

Original: English

Economic Commission for Europe

Steering Committee on Trade Capacity and Standards
Working Party on Regulatory Cooperation and Standardization Policies session

Twenty-eighth session
Geneva, 14–16 November 2018
Item 9 (b) of the provisional agenda
International regulatory cooperation: Sectoral projects

Draft proposal for a common regulatory framework on cybersecurity

Submitted by the secretariat

Summary

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

This first discussion will seek the opinion of delegates on the direction taken by the proposed common regulatory framework. If their opinion is favourable a final proposal will be submitted for the Working Party 6 annual meeting in 2019.

Proposed decision:

"The Working Party expresses its favourable opinion regarding the overall approach of the common regulatory framework as contained in this draft proposal.

It requests that the proposal be further refined; work on its finalization be entrusted to the Group of Experts on Regulatory System and the secretariat; and a more mature draft be submitted for the Working Party 6 annual meeting in 2019. It also requests the secretariat to continue to report on the progress of the initiative.

GE.18-14944(E)
1814944

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 the IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE), which have been actively supporting the project.

3. Discussions were held and drafts proposals for a common regulatory framework in cybersecurity were presented to two meetings of the Group of Experts on Risk Management in Regulatory Systems (March 2018 and July 2018).

4. This document presents a first draft for a common regulatory framework in this sector.

II. Objectives of the common regulatory framework

5. The purpose of the sectoral initiative on cybersecurity is to promote the convergence of national technical regulations currently in place, or yet to be put in place, in this sector towards a shared framework that is based on a risk-based approach and other international best practices. This will reduce barriers to trade for components, equipment, qualified persons and services, will encourage competition, increase market choice and will reduce costs. It will also increase the level of data protection for banking, health and other essential data services and the level of reliability, continuity, safety and security of critical infrastructures, such as electrical energy supply, and other essential services that are the backbone of any national economy. It will therefore help to ensure the general wellbeing and prosperity of a country's citizens.

6. More specifically, the common regulatory framework will:

- Promote a globally harmonized legislation.
- Promote legislation which is proportionate to the risks it was set out to address.
- Ensure mutual acceptance of test and assessment procedures and results among the test houses.
- Strive for consistent and comparable procedures for the assessment and implementation of actions for cybersecurity.

III. Background

7. In the digital era, cybersecurity is an essential element for the economic competitiveness and security of most of the world's economies.

8. Guaranteeing a high level of cyber resilience across the world is of paramount importance for ensuring essential services and achieving consumer trust in the digital era, and for the further development of a safer, more innovative, competitive, sustainable and affluent world.

9. Cyber threats are a worldwide phenomenon that crosses national, regional and international borders. Cybersecurity therefore requires an integrated approach at all levels.

10. To be efficient, cybersecurity measures on business, national and international level should be based on results of a systemic risk management process, with involvement of all relevant stakeholders.

11. The basic principles for cybersecurity are well documented in many international standards, but are not well known, understood or applied. Examples are the IEC 62443 series and the International Organization for Standardization (ISO)/IEC 27000 series of international standards.

12. There is confusion between the needs of cyber physical applications, so called Operations Technology systems, such as critical infrastructure and smart systems, and the need to keep those systems running in the real world, and those of purely informational systems, so called Information Technology systems, with the need to protect data and keep it flowing securely in the virtual world.

13. It is apparent that cyber protection of a technical system needs a systems-wide approach. It is apparent that a risk-based approach is needed for the following reasons:

- In any system some elements are more valuable or more vulnerable than others and need stronger, more costly protection, while other elements can be afforded lesser, lower cost protective measures. This analysis should be based on risk.
- A balance is needed between the level of protection and the cost of protection.

14. It is apparent that, in a systems approach, stronger and lesser forms of protection are appropriate, which means that stronger and less forms of confirming that the protective requirements have been met is also appropriate.

15. It is therefore apparent that a holistic cybersecurity approach should be neutral with respect to conformity assessment and accommodate different forms of conformity assessment – 1st party, 2nd party and 3rd party conformity assessment – according to the different levels of risk determined for the different system elements being protected.

16. Since cyber threats can be nationally, regionally or internationally based, international best practices are most appropriate. The ISO and IEC International Standards are increasingly adopted by countries at the regional and national level, either in full, without any variation, or in part, with supplementary requirements contained in national standards.

17. Countries use standards in their regulations in different ways, including:

- by making standards mandatory through a legislative act;
- by making compliance with the standards a means of proving compliance with the essential requirements laid out in the legislation; under this approach, equipment, people qualifications, services, practices and processes that comply with the provisions of the standards are “deemed to comply” with the requirements specified in the regulations.

18. When the risk analysis determines that 3rd party conformity assessment is appropriate, it shall be advised to use international best practices and to employ global certification services such as offered by the IECEE, when available and appropriate.

IV. Scope statement of the Common Regulatory Objectives

19. The Common Regulatory Objectives (CROs) presented in this document have been drawn up in accordance with Recommendation L of the Working Party on Regulatory Cooperation and Standardization Policies (Working Party 6) of the United Nations Economic Commission for Europe (ECE/TRADE/378 – ECE Recommendations on Standardization Policies).

20. The purpose of the CROs is twofold. On the one hand, they can be used as a model to draw up legislative instruments in countries that do not currently have regulations in this sector. On the other hand, they can be used to align existing national regulation with an internationally harmonized best practice.

21. The CROs are drawn up with reference to international standards and conformity assessment procedures developed by IEC and ISO and to best practice in the assessment of conformity to such standards, within the IECEE.

22. The CROs address a systematic methodology for determining an appropriate level of requirements and conformity assessment based on risk.

23. The CROs address the requirements for system's technology including components, products and equipment, and for the competency and qualifications of persons, and for the management processes including, component design, systems integration and realisation, operation, maintenance, upgrade, and so on (CROs – Part 4 of the present document).

24. Cybersecurity can be assured through a variety of legitimate means. The present document describes a systematic methodology for a systems approach to cybersecurity. It is different from other methodologies in that in addition to modelling the technical system, carrying out a risk analysis and a requirements gap analysis, it also includes an analysis of the conformity assessment needs. It is also, and has to be, a flexible methodology because it has to be applicable to many varied technical systems.

25. Additionally, the present document is based on the life-cycle approach, which requires proper inspection, maintenance, repair and upgrade of the technical system. This approach guarantees effective and efficient cybersecurity over time as the system itself evolves and as the nature of the threat evolves.

26. A national regulatory framework can use this model, itself, for certain critical sectors and applications, or require that the commercial players in those same sectors and applications, or others, use the model to satisfactorily demonstrate compliance. Third party conformity assessment should only be required where appropriate, according to the results of the risk analysis.

27. Converging onto a common methodology based on harmonized international standards and international conformity assessment best practices presents several advantages. Among others, when third party conformity assessment is used to demonstrate conformity of components and technology, people competency and qualifications, recognition of this conformity in international trade and the movement of qualified persons, is facilitated.

28. Conversely, the existence or use of disparate requirements and procedures in sectors that operate as truly global and integrated applications may, in and of itself, constitute an increased risk.

29. For these reasons, when third party conformity assessment is required, an internationally recognized certification scheme, such as the IECEE, is of essential importance in order to reduce unnecessary costs associated with duplication of inspection, assessment, qualification and testing.

30. One final and essential element of the present document relates to market surveillance. Market surveillance is necessary to monitor the proper application of the CROs by industry and increase confidence in the effectiveness of the CROs. Common guidelines will be defined to support the national authorities defining and implementing actions and procedures, including for the removal of non-compliant system components and products from the national market.

V. Common Regulatory Objectives

1. CROs – Part 1: Methodology for achieving appropriate cybersecurity – an overview

31. This common regulatory framework describes a comprehensive and systematic methodology for a systems approach to cybersecurity. This generic methodology has 5 steps which are then periodically repeated. The five steps are:

- Risk analysis and risk rating;
- Requirements – standards gap analysis (Part 4 of the present document);
- Conformity assessment analysis according to the risk rating (Part 5 of the present document);
- Application – demonstration of compliance;
- R3 – review, revise, renew.

2. CROs – Part 2: Methodology for determining appropriate Requirements

32. Gap analysis – the generic matrix model (see Annex A) is used to determine the points at which requirements are needed for a system. The analysis of different systems in different situations will lead to different needs for requirements. Requirements will be based on international standards such as those of the IEC and ISO (as given in Part 4 and listed in the Appendix to this document), or, if not available, then on regional standards or finally on national standards. Where no standards are available requirements should be based on market accepted best practices and procedures.

33. The ECE Working Party 6 Recommendation R "Risk Management in Regulatory Systems" should be used by regulatory authorities to ensure consistency and proportionality between the existing cybersecurity risks and respective regulatory requirements.

3. CROs – Part 3: Methodology for determining appropriate Conformity Assessment Requirements

34. Risk analysis – the generic matrix model (see Annex A) is used to determine the points at which requirements are needed for a system. The method for determining which requirements are appropriate is given in part two of this document. The level of conformity assessment that should be applied to the requirements will be determined by means of a risk assessment resulting in a risk rating of each point on the generic matrix model. The analysis of different systems in different situations will lead to different risk ratings. High value points will afford higher levels of conformity assessment, as will high vulnerability points, while lower value and lower vulnerability points can afford lower levels of conformity assessment.

4. CROs – Part 4: Requirements for acceptance in the market

A. Requirements for components, products, equipment

35. Requirements for components, products and equipment used as system elements will be based on international standards such as those of the IEC and ISO (as given in Part 4 and listed in the Appendix to this document), or, if not available, then on regional standards or finally on national standards.

B. Requirements for personal competency

36. Requirements for personal competency will be based on international standards such as those of the IEC and ISO (as given in Part 4 and listed in the Appendix to this document), or, if not available, then on regional standards or finally on national standards. Where no standards are available requirements should be based on market accepted competency.

C. Requirements for processes

37. Requirements for processes will be based on international standards such as those of the IEC and ISO (as given in Part 4 and listed in the Appendix to this document), or, if not available, then on regional standards or finally on national standards.

5. CROs – Part 5: Reference list to international standards providing the presumption of conformity with this regulation model

38. Standards providing the presumption of conformity with the requirements in Part 4 are listed in the Appendix, chapters A, B and C. The list of standards is to be updated as frequently as necessary depending on the publication output of IEC or ISO/IEC International Standards relevant to the objectives of this regulation model.

39. Subject to appropriate review by the ECE management and governance bodies, the group of countries that have implemented this regulation model shall form an ECE Standard Acceptance Group which will concern itself with the acceptance of IEC or ISO/IEC International Standards providing the presumption of conformity with this regulation model. The members of this group seek for access to all standardization work of IEC (drafts, meetings) in order to influence standardization with concerns of regulators in an early stage. After the group has accepted it, the standard will be listed in the Appendix to this regulation model. If there is a former edition of the standard, this former edition will be withdrawn from the list within three years.

6. CROs – Part 6: Requirements for conformity assessment

A. Definition of applicable conformity assessment procedures

40. Compliance with the CROs shall be by an appropriate means of conformity assessment against requirements as specified in the specific application as determined by the process given in part one of this document.

41. When third party conformity assessment is required, compliance with this CRO shall be by use of an international certification scheme such as the IECEE for direct market acceptance of products, persons, services and organizations carrying IECEE Certification. Alternatively, where national legislation does not allow for use of IECEE Certificates, national certification of compliance should be based on IECEE testing, inspection and assessments.

B. Recognition of conformity assessment bodies

42. The accreditation of conformity assessment bodies and test laboratories must follow the applicable ISO/IEC International Standards (see Appendix, chapter D.1). The accreditation body must be a member of International Laboratory Accreditation Cooperation/International Accreditation Forum. At least one member of the assessor team needs competence in the respective cybersecurity requirements (see e.g. the list of approved IECEE Assessors).

43. Certificates must be in line with the requirements of the respective scheme type as described in the applicable ISO/IEC standard (see Appendix, chapter D.2).

44. The use of the IEC Conformity Assessment System IECEE provides the presumption of conformity with the requirements of Part 6.

7. CROs – Part 7: ECE Cybersecurity Steering Committee

45. Subject to appropriate review by the ECE management and governance bodies, in order to monitor the implementation of the CROs in the countries that have based their national legislation on the ECE regulation model and to update the regulation model in the light of their experience, the ECE Cybersecurity Steering Committee is to be formed and operate under the umbrella of ECE Working Party 6.

46. The Cybersecurity Steering Committee agrees on a constitution and other governing rules and procedures of the daily operations (e.g. voting procedures).

47. The Cybersecurity Steering Committee notifies the members of the ECE Standard Acceptance Group.

48. Members of the Cybersecurity Steering Committee with the right to vote are the representatives of those countries having implemented the regulation model. Observers who are also invited to attend the meetings are: representatives from IEC Standardization Management Board, IEC Conformity Assessment Board, IEC Technical Committee 65, ISO/IEC Joint Technical Committee 1/SC27, IECEE, IEC System for Certification to Standards Relating to Equipment for use in Explosive Atmospheres, the ECE Advisory Group on Market Surveillance.

8. CROs – Part 8 - Market surveillance

49. Subject to appropriate review by the ECE management and governance bodies, in order to monitor proper compliance with the requirements of this model regulation in the marketplace, a network of market surveillance experts in cybersecurity is to be formed and operated (see Appendix, chapter F.1).

50. Planning of market surveillance processes should be based, inter alia, on the ECE Working Party 6 Recommendation “S” on applying predictive risk management tools for targeted market surveillance.

51. In case of critical non-conformance, an international alert system should be put in place to inform all ECE member States about recently detected risks.

Appendix
List of accepted standards and guidelines under maintenance of the ECE-IEC-ISO

A.1. Basic concepts and methodology

1. To be further developed

A.2. Design requirements for system components

2. To be further developed

A.3. Production of equipment

3. To be further developed

B.1. Personnel competency requirements

4. To be further developed

D.1. Conformity assessment standards

5. ISO/IEC 17065, ISO/IEC 17021, ISO/IEC 17024, ISO/IEC 17025

D.2. Fundamentals of product certification

6. ISO/IEC 17067

F.1. Guidelines for market surveillance

7. Guidelines for market surveillance are in preparation by this sectoral initiative in cooperation with the Advisory Group on Market Surveillance.

Annex A

Explanation of the Generic Matrix Model

1. The Generic Matrix Model (GMM) is a tool used to model a technical system and then to cross-reference that model with objects of conformity (or the things that can actually be assessed for conformity against requirements). The GMM is usually represented as a matrix with the system modelled vertically down the left-hand side and the objects of conformity listed across the top.

2. In a graphical representation of the GMM, horizontal lines are drawn from the system-model features across the page under the objects of conformity. Similarly, lines are drawn vertically downwards from the objects of conformity. The intersection points of the vertical and horizontal axes are where conformity assessment can be done against requirements, if the requirements are available.

3. The GMM can be used to determine what is important for a given technical system when viewed through a specific lens. This will determine the most important features and sub-features that should be visible through that lens and that therefore should be apparent in the system-model. When cybersecurity is being viewed through the lens, the system may be modelled with such features as technology or components, interconnections, interventions, security zones, intrusion testing, and so on.

4. The requirements could be many things depending on what it is that is trying to be achieved. Typically, requirements come in the form of best practices, qualifications, specifications, standards, a certain minimum or maximum result on standardized tests, and so on. To achieve the requirements, it may also be necessary to have a certain type or level of equipment, knowhow, skill-sets, competency, experience, and so on.

5. The act of making an assessment to see if the requirements have been fulfilled is the act of assessing conformity to the requirement. The formal term is conformity assessment . There are essentially three possible objects of conformity. They are products, people (competencies) and processes.

6. These three objects of conformity are the basic three. Many other objects of conformity have been proposed, such as services, data, installations, projects, bodies or organization, and systems. But in reality, each of these is simply one or a combination of the three basic. For example, services are essentially just processes, performed by people (with the appropriate competencies), perhaps using appropriate products or equipment. There is nothing else. Therefore, services are already covered by the three basic objects of conformity and do not need a special category of their own.

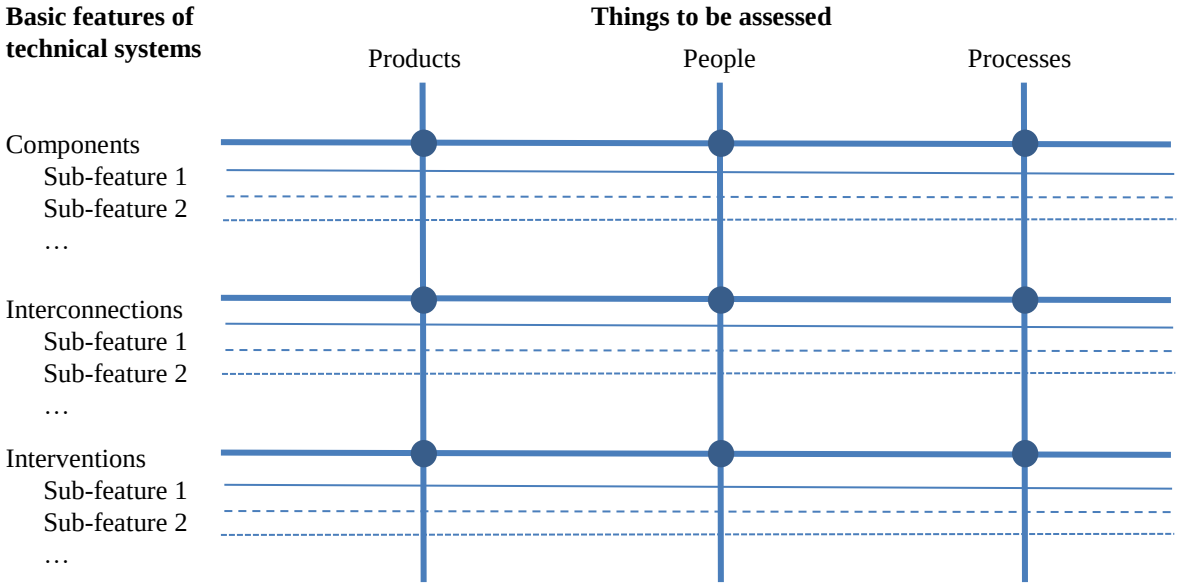
7. This having been said, if it serves a sector to specify more than the three basic objects of conformity, then the additional(s) object(s) of conformity should be included in the specific GMM.

8. At the intersection points of the system-model features and the objects of conformity is where the requirements can be applied. What the requirements are and whether they are available will be determined through a gap analysis.

9. Understanding the system, knowing where the value is and where the vulnerabilities are will then be used with a risk assessment of each of the intersection points to determine what kind of conformity assessment is needed against the requirements at each point. High value or high vulnerable intersection points will need stronger conformity assessment, while lower value or lower vulnerability points will need lesser conformity assessment. The full

range of conformity assessment options should be available for appropriate use. This means first party conformity assessment such as manufacturer's or supplier's declaration of conformity; second party conformity assessment such as self-assessments and internal audits by the user or owner of the system; and third-party conformity assessment such as type 1 (ISO/IEC 17067) type-testing, or type 5, full certification of conformity, and so on. Most regulations should be neutral in terms of conformity assessment, and only specify what is appropriate according to the results of the risk analysis.

10. The vertical and horizontal intersection points of the GMM are where conformity assessment is done, and systems-approach is the overall matrix of requirements and conformity assessment activities.



Generic model of a system's approach to conformity assessment (simplest form)

What is a technical system?

11. A technical systems are not natural systems such as biological systems like the blood circulatory system, or environment systems like the weather system, or celestial systems like the solar system, etc, rather, technical systems are man-made systems.

12. What are the commonalities between railway systems, cloud computing, the smart grid, industrial control systems, a nuclear power plant and electric distribution system, an oil refinery, a gas distribution system, a health information system, smart homes, and so on?

13. They are all technical systems.

14. Now, if a technical system is considered to be

- a group of interacting, interrelated, or interdependent elements forming a purposeful whole;
- and that those elements can be procedural, physical and/or virtual;
- and that those elements can be components that need to be designed and manufactured or created;

- and that the system itself will be designed and built (or systems-integrated) and that the elements of the system can be confined to a limited physical location, or can be spread out over a large physical distribution;
- and that those elements need periodically to be revised, maintained and/or updated/upgraded;
- and that some of those elements transmit and receive information between themselves;
- and that the system is in some way connected to the world beyond the system itself, either physically or virtually (eg: via the internet);
- and that the whole system itself is periodically or constantly undergoing modification and development through interventions that could be virtual, automated or human;

then, all technical systems are quite generic.

15. Although technical systems are quite generic, they are also quite complex and confusing. Therefore, to simplify, all technical systems can be considered as consisting of three basic features: Components, Interconnections and Interventions

16. These three features, as listed, are somewhat chronological in the lifecycle of a system, occurring one after the other. For example, components are designed and build, then systems-integrators design the system, select the components, and then realise the system. The system is then operated through interventions. Each feature follows the other. But there are also many loop-backs. As a system ages and evolves, new and replacement components are needed often with new designs and technologies, thus looping back to the components feature. The system itself may evolve with new or different needs requiring new types of components, concepts and technology to be integrated, thus looping back to the interconnections feature. And as operational practices evolve and improve, new and different types of interventions are required over time.

17. Components: Every technical system has components which are physical but can also be virtual (such as control software, or data, etc). Each component has a purpose and a reason to be part of the system. Components need to be designed for their purpose and then realised (manufactured, developed, etc). Components sometimes need to be repaired, upgraded or replaced. Sometimes there can be a long lead-time (interval) for components, between realisation and integration into a system (the shelf-life). This lead-time needs to be managed to ensure the integrity of the component and the system.

18. Interconnections: This is the systems integration. It is how the components interact, communicate and work together. This can be physical interconnections such as parts moving through a manufacturing system, or trains on tracks, or transmission wires carrying electricity, or cables carrying control signals. It can be information flows through cables or wireless. The tracks, transmission wires and signal cables would all be components, but their function of carrying trains, electricity and signals, is the interconnection.

19. The systems integration needs to be designed, and sometimes the interconnections need to be repaired, upgraded or replaced. In some situations, the interconnections can be changing dynamically, all the time, such as the internet, and the smart grid (with new generating capacity and new loads coming-on and going-off in an uncontrolled organic development, all the time).

20. Interventions: These can be human, virtual or automatic. Interventions are mostly involved with the operations of the system throughout its lifecycle, and can include best practices, processes and procedures. They can also involve services provided internally or out-sourced, such as vender services. Some interventions can be automated such as the automatic upgrading of anti-virus/hacking protection software in IT systems, or the automatic handshaking and virtual certificate control of incoming data. Often interventions are

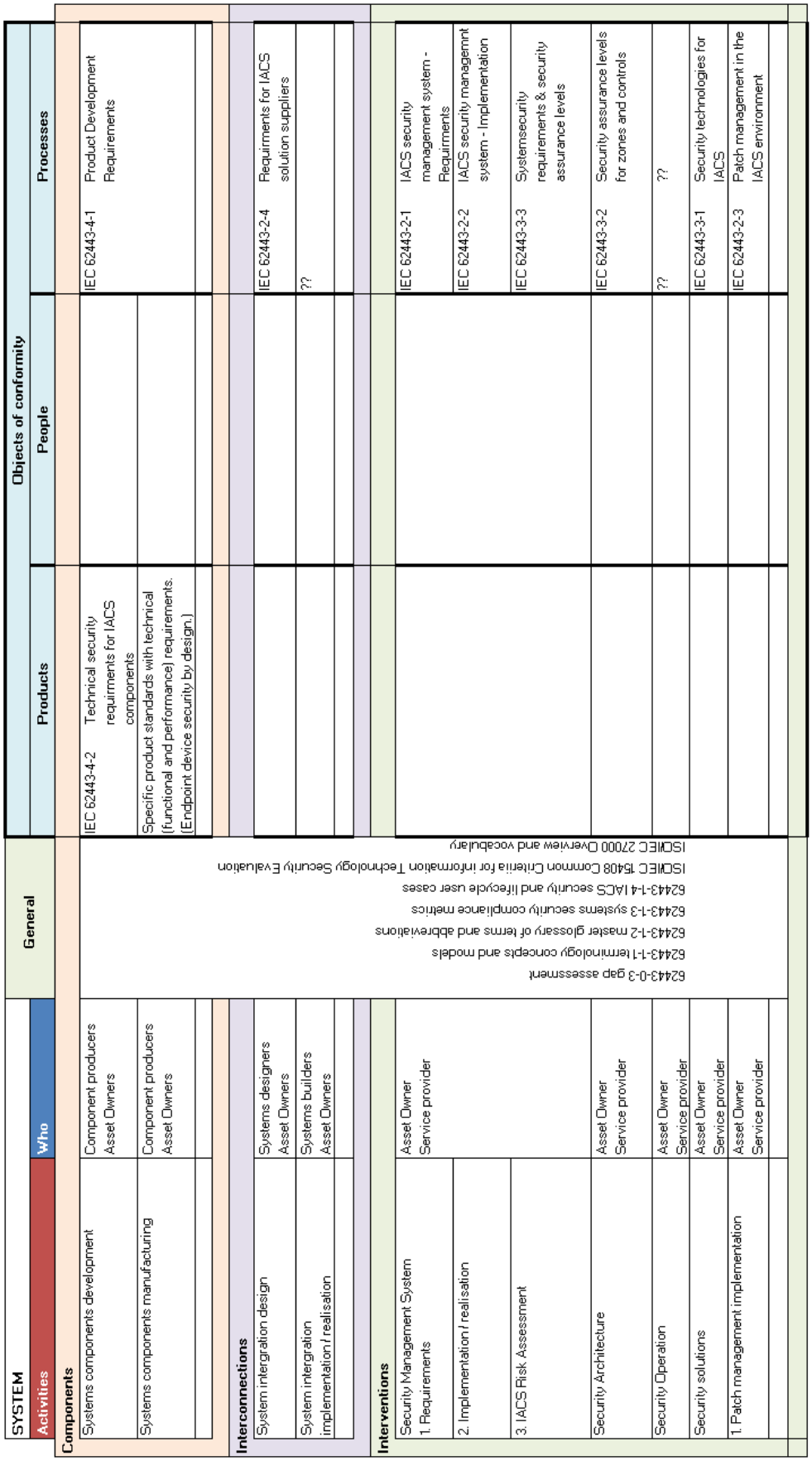
mundane but important human best practices such as regularly changing passwords, or reporting and cancelling lost passkeys or badges, etc.

21. This concept of three basic features is the very high level, generic view of a system. Below each of these three features there will always be sub-features that provide greater detail about the system. Many of the sub-features will be the same from one system to another, but their individual importance may differ greatly from one system to another. And some systems will have sub-features that are unique to that particular system. Depending on the level of detail required, a large number of sub-features may be defined, and even sub-categories within some of the sub-features.

Annex B

Examples of the Generic Matrix Model used in different application sectors

Industrial automation GMM in table format.



SYSTEM		General	Objects of conformity			
Activities	Who		Products	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 standards with technical (functional and performance) requirements. (Endpoint device security by design.)			
Interconnections						
System intergration design	Systems designers Asset Owners				IEC 62443-2-4 Requirments for IACS solution suppliers	
System intergration implementation / realisation	Systems builders Asset Owners				??	
Interventions						
Security Management System 1. Requirements	Asset Owner Service provider	62443-0-3 gap assessment 62443-1-1 terminology concepts and models 62443-1-2 master glossary of terms and abbreviations 62443-1-3 systems security compliance metrics 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			IEC 62443-2-1 IACS security management system - Requirments	
2. Implementation / realisation					IEC 62443-2-2 IACS security managemnt system - Implemenitation	
3. IACS Risk Assessment					IEC 62443-3-3 Systemsecurity requirements & security assurance levels	
Security Architecture	Asset Owner Service provider				IEC 62443-3-2 Security assurance levels for zones and controls	
Security Operation	Asset Owner Service provider				?? ??	
Security solutions	Asset Owner Service provider				IEC 62443-3-1 Security technologies for IACS	
1. Patch management implementation	Asset Owner Service provider				IEC 62443-2-3 Patch management in the IACS environment	