	CAB/1737A/R
For IEC use only	
	2018-05-24

INTERNATIONAL ELECTROTECHNICAL COMMISSION

CONFORMITY ASSESSMENT BOARD (CAB) **Meeting 43, Geneva, 2018-06-11**

SUBJECT **Agenda item 6.5**

Updated report from CAB WG 17 - Cyber Security

TERMS OF REFERENCE

- To investigate the market need and timeframe for CA services (global certification schemes) for products, services, personnel and integrated systems in the domain of cyber security.
  - Excluding the scope of Industrial Automation Applications covered by IECEE CMC WG cybersecurity.
- To communicate to other industry sectors the generic Cyber Security approach taken by IECEE CMC WG cybersecurity and how this may apply to those other sectors.

BACKGROUND

This updated version includes, in Annex B, the CAB comments received.

Since the Vladivostok CAB meeting, held last October, WG 17 met on 28 January 2018, in Frankfurt (DE). The group is due to meet again on 12 June 2018, just after the Geneva CAB meeting.

The report is in three parts:
Part A – Recommendations submitted to the CAB for formal approval: none
Part B – items of interest to the CAB
Part C – Review of previous CAB Decisions Related to this subject

Annex A: WG 17 minutes of the January meeting
Annex B: CAB comments received

EXECUTIVE SUMMARY

Following the CAB/WG 17 meeting in Frankfurt, on 2018-01-28, several actions have been taken mainly focused on the following points:
- push the recognition of IEC standards and schemes at the EU level in the Cybersecurity Certification Framework. All members of CAB WG17 involved in the EU work are doing it;
- continue to work on the Matrix Approach;
- establish a list of relevant events where the IEC Cybersecurity schemes could be promoted;
- initiate the links with UNECE.

ACTION

Members of the CAB are invited to review this report, and comments received, for discussion at the June CAB meeting.

Part A: recommendations for CAB approval

There is no formal recommendation coming from the WG 17 for this June 2018 meeting.

Part B: items of interest to CAB

The last WG 17 report from January 2018 meeting is included, as Annex A, for your information:

B.1 Follow-up actions since the January meeting

During the last 2,5 months the assigned tasks have not been concluded. However a lot of influence work has been done at the European level through the professional associations and directly to the institutions (European Commission, European Parliament) by some members of WG 17 and also by colleagues in our respective companies. This work is still ongoing as we are in a very busy period regarding the regulation proposal.

B.2 IEC e-tech article

The article expected in e-Tech has still not been published due to the retirement of one of the key people from IEC. We are still pushing to get this final article published in a next edition of the e-Tech.

B.3 Industry sectors

Information from different industry sectors has been collected thanks to the participation of the CAB Secretary, David Hanlon, in some events related to Cybersecurity.

Part C: review of Previous CAB Decisions Related to WG 17

Decision 35/8 — *CAB WG 17 – Cyber Security*

The CAB, recognises the need for additional evaluation / consideration of cyber security opportunities across the IEC and its CA Systems, decides to create a new working group, WG 17 with Mr Ron Collis as convenor, to investigate the market needs for possible CA services in Cyber Security, and tasked to report back to CAB at its next meeting in November.

Decision 36/13 — *WG 17 - Cyber Security*

The CAB thanks WG 17 for its document, CAB/1316/R, notes and endorses this report. The CAB also requests WG 17 to map out relevant CA needs in the overall area of cyber security across IEC market and stakeholder groups and to come back to CAB with a proposed plan by the next CAB meeting in June 2015. At the same time, the CAB supports the continued work of IECEE on Industrial Automation in this area to address more immediate cyber security needs of the Industrial Automation Industry and encourages the IECEE to continue the advancement of that work. CAB requests that CAB WG 17 monitors the IECEE work on cyber security.

Decision 37/21 — *CAB WG 17 – Cyber Security*

The CAB thanked WG 17 for its report, CAB/1383/R, noted that its scope is focused on home automation, smart devices (such as smart meters) and medical devices, and indicated that WG 17 should focus on all those sectors concerned with cyber security except those currently being worked on in IECEE (industrial automation).

Decision 38/14 — *CAB WG 17 – Cyber Security*

In the absence of the WG 17 Convener CAB thanked the CAB Secretary for his verbal report of the meeting held in Frankfurt the week prior to this meeting, and look forward to receiving the formal report after this General Meeting.

Decision 39/01 — *CAB WG 17 – Cyber Security - new* scope (by correspondence)

CAB agreed to the following new scope for WG 17:

- To investigate the market need and timeframe for CA services (global certification schemes) for products, services, personnel and integrated systems in the domain of cyber security.
  - O Excluding the scope of Industrial Automation Applications covered by IECEE PSC WG 3 Task Force on Cyber Security.
- To communicate to other industry sectors the generic Cyber Security approach taken by IECEE PSC WG 3 Task Force on Cyber Security and how this may apply to those other sectors.

Decision 39/23 — *CAB WG 17 – Cyber Security*

The CAB thanked WG 17 for its report, CAB/1504A/R, and the CAB Secretary, Mr David Hanlon, for his role as interim Convener and accepted the offer by Pierre Selva to send a proposal for how to manage the convenership. CAB also urged the WG to move forward quickly on its outstanding actions, and approved a modification to the current scope replacing "IECEE PSC WG 3 Task Force on Cyber Security" with simply "IECEE CMC WG cybersecurity".

Decision 40/01 — *CAB WG 17 – Cyber Security - new Convener (by correspondence)*

CAB appointed Mr Pierre Selva as the WG 17 Convener, approving his proposed support team consisting of Mr Didier Giarratano, Mr David Doggett and Mr David Hanlon (CAB Secretary), and urged this new team to quickly start to move WG 17 forward to the completion of its assigned tasks.

Decision 40/12 — *CAB WG 17 – Cyber Security*

The CAB thanked the new WG 17 Convener, Mr Pierre Selva, for the report, CAB/1565/R, and encouraged the new Convener to move the tasks of this working group forward quickly.

Decision 41/26 — *Report from CAB WG 17 – Cyber Security*

The CAB thanked the Convenor, Mr Pierre Selva, for the report given in document CAB/1626/R and urged the group to move quickly toward a situation where it could make concrete recommendations.

Decision 42/12 — *CAB WG 17 – Cyber Security*

The CAB thanked the WG 17 Convenor, Mr Pierre Selva, for his verbal report and thanked the German NC for their proposal given in document CAB/1679/DC, with comments in CAB/1679A/CC. CAB recognized that efficiency could be gained by concentrating all IEC operational CA cybersecurity activities.

To serve the needs of the market and regulators, IECEE shall serve as the focus point for technical evaluation forming part of the conformity assessment services for all IEC CA Systems. The other IEC CA Systems shall define any additional sector-specific requirements as far as appropriate.

The CAB recognized the importance to maintain a strong contact and relationship with UNECE with the goal of creating a Common Regulatory Objectives best practice document for use by regulators, as was created with IECEx in 2011.

IEC CAB WG 17 Frankfurt 20180129
Meeting Report
2018-03-09

IEC Conformity Assessment Board (CAB)

IEC CAB WG 17 2018-01-29 Frankfurt
Cybersecurity

Meeting Date	29th of January, 2018
Meeting Place	VDE, Frankfurt

Present

Giarratano, Didier
Hanlon, David
Imgrund, Gerhard
Kajiya, Toshiyuki
Kreuter, Beat
Pauslen, Shawn
Selva, Pierre — Convenor
Walch, Otto

On Remote

Margis, Steve
Nash, Mike
Yamada, Tsutomu
Suárez Giovanni Cambronero

Some Abbreviations

CI = Critical Infrastructure
CS = Cyber Security
GS = General Secretary
SDO = Standards Development Organization, or
Secure Development Organization
SDL = Secure Development Lifecycle
NIS = National Infrastructure

1 Opening of meeting

Opening by the convenor at 10:00 local time.
Welcome and introduction.
Short roundtable to know who was present.

2 Review of last meeting minutes

Approval of the agenda (on Collaborative tool).

3 Appointment of a secretary for the meeting

The secretary duties were shared between the Convenor and David Hanlon.

4 Objective of the meeting

Specific focus on European Cybersecurity Scheme proposal and work on Matrix prepared by David.

5 Remember the CAB WG 17 terms of reference

To investigate the market need and timeframe for CA services (global certification schemes) for products, services, personnel and integrated systems in the domain of cyber security.

- Excluding the scope of Industrial Automation Applications covered by IECEE CMC WG cybersecurity.

To communicate to other industry sectors the generic Cyber Security approach taken by IECEE CMC WG cybersecurity and how this may apply to those other sectors.

6 European Cybersecurity Certification Scheme proposal

The full proposal is available at the following link.
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0477&from=EN

Ideas to share : Technical and detailed explanation of the proposal / How to get a Mutual Recognition of our IEC Certification scheme dedicated to Cybersecurity by the European Commission ?

This proposal for regulation will reinforce the role of ENISA, the European Union Agency for Network and Information Security.
Objective of WG 17: be sure the ENISA will reference the International Standards (IEC/ISO) and will recognize the test report issued under our schemes.

Didier Giarratano made a presentation on the main stakes of this proposal:

Domain	Corporate infrastructure	ICT Side (equipment)	ICS Side (Electrical distribution, Process, Product related)
Energy (electricity, oil, gas, smart)	ISO/IEC 27001 ISO/IEC 27019	Not required at that stage	IEC 62443
Transport (air, rail, road, maritime)	ISO/IEC 27001 ISO/IEC 27002	Not required at that stage	IEC 62443
Banking	ISO/IEC 27001 ISO/IEC 27002	Common Criteria	Not Applicable
Financial Market	ISO/IEC 27001 ISO/IEC 27002	Not applicable	Not Applicable
Health	ISO/IEC 27001 ISO/IEC 27002	Not Applicable	IEC 62443
Water	ISO/IEC 27001 ISO/IEC 27002	Not Applicable	IEC 62443
Digital Infrastructure	ISO/IEC 27001 ISO/IEC 27002	Common criteria	IEC 62443(1)

Note 1: Like sensors

Attention is drawn on the wish of National agencies to be powerful to fight against attacks in the Power Grid (at least). Consequently, certification will be required.
Accreditation of test laboratory: this point is still unclear. We should promote our vision and be sure that new requirements (outside of ISO/IEC 17025) are not added.
Same level of attention to the requirements for Certification Bodies for which requirements are not known today, too.
It is also important to notice that the Common Criteria is today the most advanced Scheme worldwide, including Europe. However, this schemes is based on ISO/IEC15408 which are not the preferred standards for us. ECSO is promoting this scheme.

A lot of seminar and presentation are done now by a very diffuse range of stakeholders. Further, direct contact with the European Commission and its representatives are done at all levels.
It exists also other initiatives which seems to be “in competition” with ENISA :

- European IACS Components CS Certification framework

Not yet any connection with Enisa
https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf
https://erncip-project.jrc.ec.europa.eu/

➔ **Bert to follow up what is done at this level**

- Cybersecurity Grid Code ➔ They are not referencing the IEC Standards

- ECSO – European CS Organization → based on Common Criteria ISO/IEC 15408

The WG 17 also mentioned the ACSEC – Guide 120 - recommendation
Generic Cybersecurity standards are coming from JTC1

For sectors specific requirements → each sector TC has to develop its own requirements, based on IEC Standards.

The CASCO work is also mentioned. Steve draw the attention on the rules for voting at this level. He mentioned that UL will participate.

In order to **influence the European Proposal**, the following action is decided :
Contact with EU Commission should be made at higher level, with a filter down effect.

- We will create a position paper view from IEC
  - IEC only has global CA Services which are of higher value for stakeholders
  - IEC CA Services are supported by the WTO and aligned with TBT Agreement recommendations
  - Participant of IEC should be General Secretary, CAB Chair and WG17 convenor.
  - Participant from Commission must be selected in the coming weeks.
  - Objective is to hold this meeting in 2nd quarter of 2018.
- We want to propose a MoU between ENISA and IEC on Mutual Recognition of our Scheme and on General collaboration.
- The most active and important National Authorities should be associated to these discussions in order to get their support.

Gerhard, David and Pierre to make a first proposal of PP by mid-March.
Pierre to identify the right contact at European Level and to propose date for meeting.
CENELEC (Bernard Thies) will be informed of our action to the commission

Further, in order to promote our scheme at a global level, we will work with UNECE to create the same kind of document that has been made for IECEx.
Pierre to make first proposal in collaboration with Chris Agius.

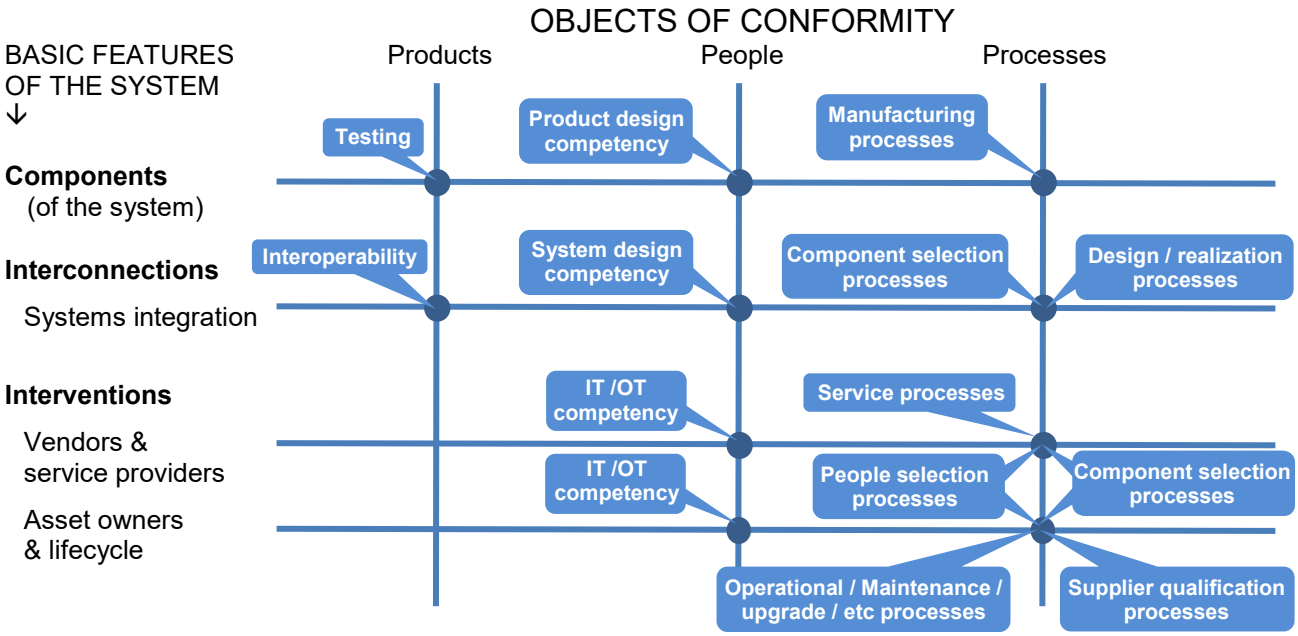
7 Matrix approach

The so called matrix approach is described in the draft document *Cybersecurity-CA-Generic-Process-02.docx* which can be found on the collaboration tools.

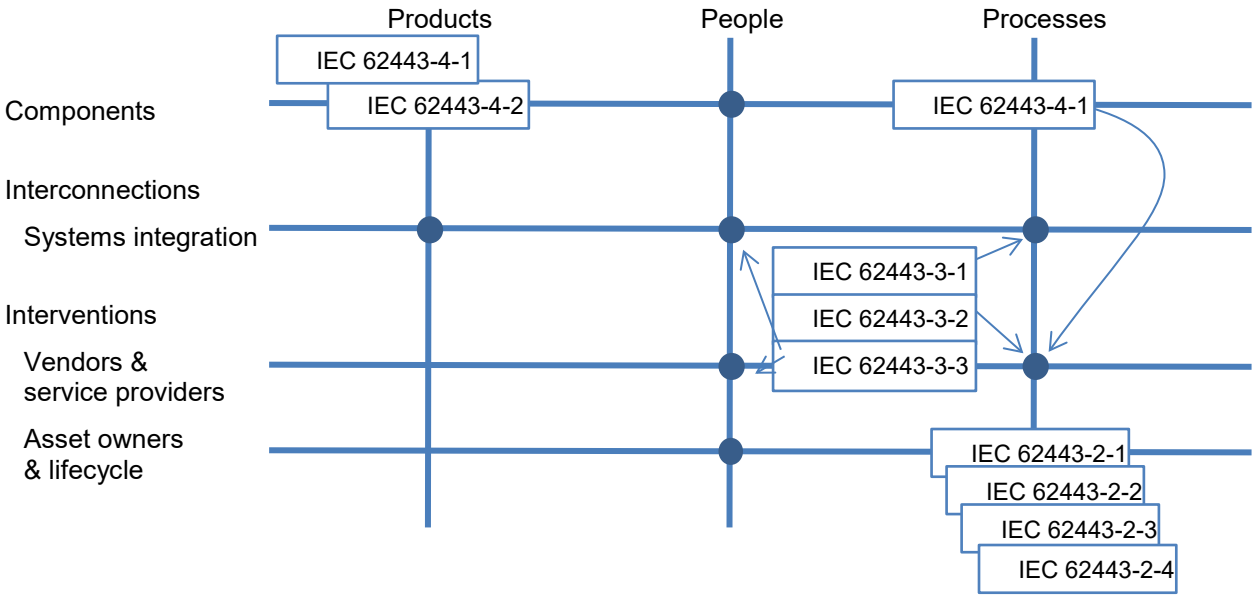
In brief it can be described as follows:
Any technical-system (as opposed to a natural system such as a blood circulatory system or a celestial system, etc.) can be modelled with three basic features being components, interconnections and interventions (normally represented as horizontal axes). Each of these features can be subdivided with sub-features to indicate important aspects of the system. The system features are then cross referenced in a matrix format against the three basic objects of conformity (things that can be certified) being products, people-competencies and processes (normally represented as vertical axes). Each intersection point, of the horizontal and vertical axes, can be assessed for importance/risk then the appropriate level of conformity assessment can be determined and applied, assuming

that the appropriate requirements or standards are available. The entire matrix is a system's-approach to CA for the technical-system.

To apply the generic matrix model (GMM) to cybersecurity, first it is necessary to determine what the characteristic sub-features of the technical–system are. Here below is a minimalist approach including components, systems integration, vendors & service providers, and asset owners & lifecycle.

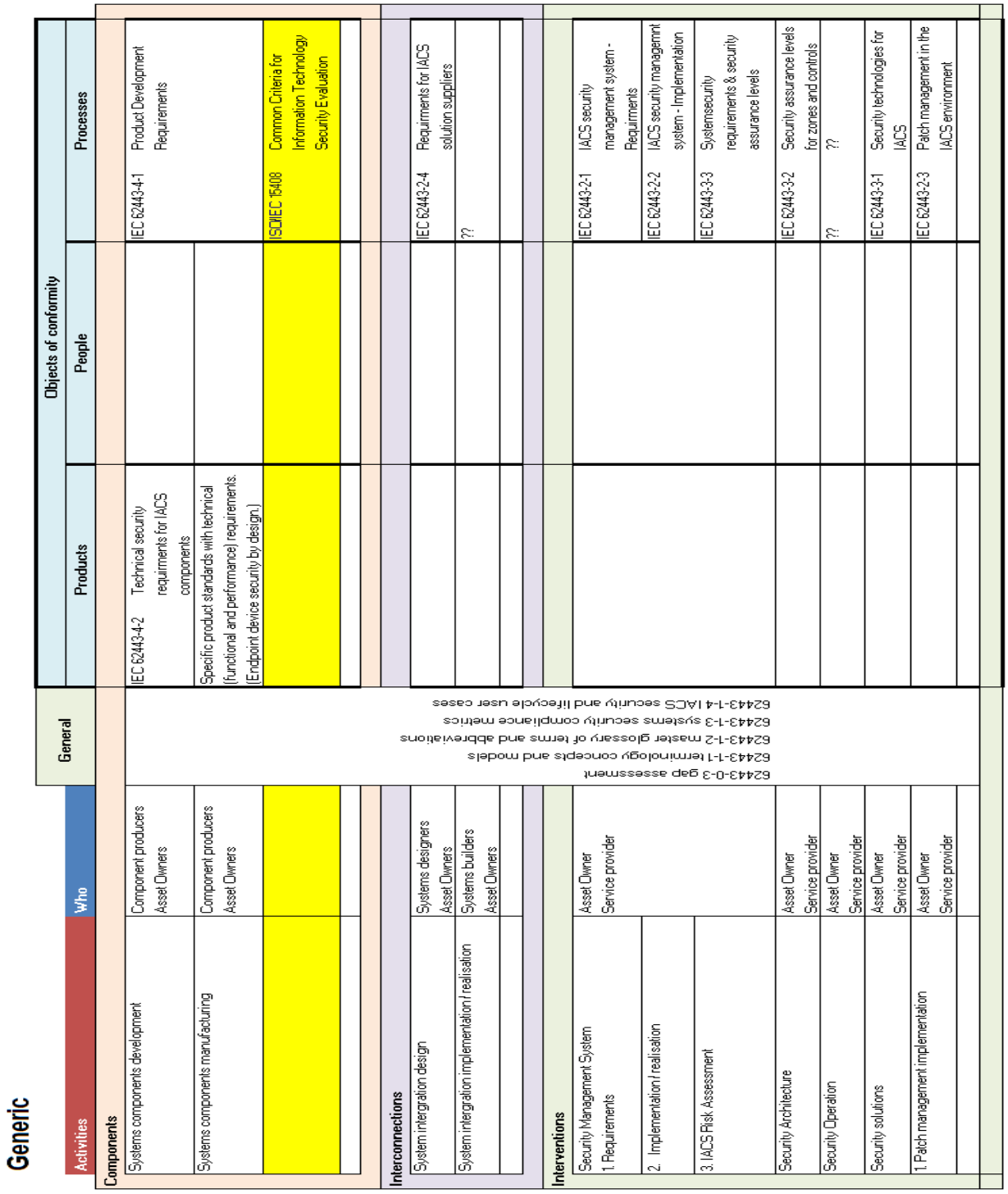


Applying the IEC 64223 series of standards to this system's-approach to CA for cybersecurity, shows that there are many gaps on the availability of standards, certainly at the product and people competency levels. It also shows that some standards may apply at multiple intersection points, and that multiple standards may apply at single intersection points.



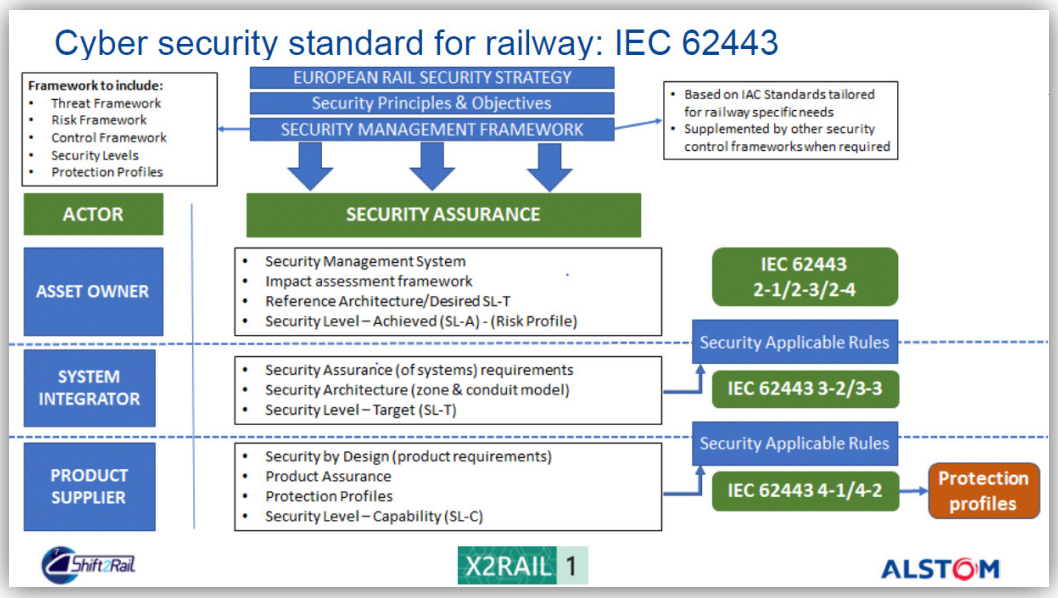
The matrix can also be expressed in a table form. In this case the intersection points will be the cells that intersect the horizontal system feature with the vertical object of conformity. The cell can then contain information about the importance/risk level as well as the required level of CA and the standard(s)/requirement(s) to be applied, and any supplementary information that is deemed important.

The table below is another variation of the GMM, as applied to cybersecurity, where the system is described in terms of activities and also shows who could be doing those activities.



Cybersecurity for Railways:

A “cybersecurity in rail” conference was held in Vienna in late November where the IEC 62443 series was indicated in a number of presentations.



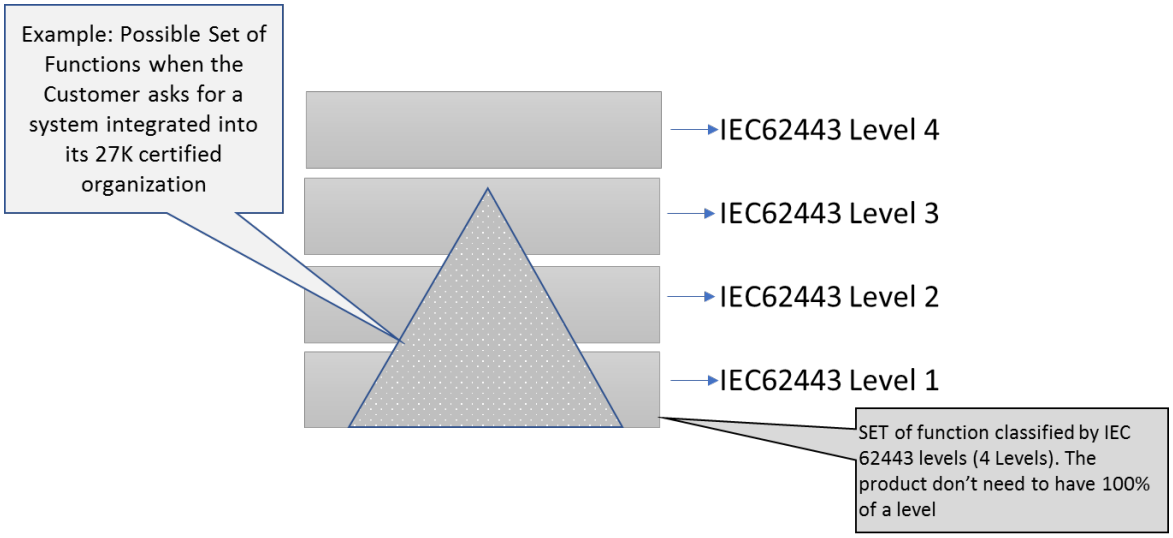
The GMM is yet to be adapted for the rail application.

Cybersecurity for Cloud Computing:

A “Certification Schemes for Cloud Computing Workshop” was held in Brussels in December where an analysis of the “controls” was done for a number of different requirements sources (including ISO/IEC 27002, C5, CSA-CCM, CCSM-ENISA). The GMM is yet to be adapted for the cloud computing application.

		Number of controls				
Controls		27002	C5	CSA-CCM	CCSM-ENISA	NIST
1)	Information Security	9	10	9	2	?
2)	Personnel & training	6	5	8	3	?
3)	Asset management	10	8	10	1	?
4)	Identity & Access	13	13	29	1	?
5)	Cryptography & key management	2	4	4	0	?
6)	Physical Infrastructure security	15	5	13	2	?
7)	Operational security	10	23	1	22	?
8)	Communications security	7	8	5	0	?
9)	Procurement management	18	14	15	2	?
10)	Incident management	7	7	3	2	?
11)	Business continuity	4	5	3	1	?
12)	Disaster Recovery	0	0	0	1	?
13)	Compliance	8	3	22	3	?
14)	Security assessment	0	3	0	2	?
15)	Device management	0	1	0	0	?
16)	Interoperability	0	5	0	1	?
17)	System security & integrity	0	0	1	4	?
18)	Risk/threat/vulnerability management	0	0	1	4	?
19)	Change & configuration management	0	0	0	4	?

ISO/IEC 27002
C5 Cloud Computing Compliance Controls Catalogue
CSA-CCM Cloud Controls Matrix
CCSM-ENISA Cloud Certification Scheme Metaframework
NIST SP-800-53 Security & Privacy Controls for Federal Information Systems & Organizations



8 Any other business

Follow up of decisions taken at Vladivostok (October 2017)

8.1 Proposal to work on a matrix by business for some representative sectors

It is requested to each individual(s) mentioned on each sector to make a first draft of the matrix at each national level with the help of local experts. Then these drafts will be proposed and shared with the entire WG17 members. This will allow checking the relevance of the matrix in each country where we have members.
It is requested to fill in these matrixes for February 2018.
Update on January 2018: take example of the first proposal made by David to create matrix for other sectors. When Matrix are ready, they must be shared with Customers and National Authorities to validate relevance. To take these presentations as opportunities to propose MoU or Recognition Agreement. This has to be done for the countries identified on point 8.3

October 2017.
Representative sectors:

- Smart Energy link with IEC SyC Smart Energy WGs 3 & 6.
  → Pierre

- Critical infrastructure (Oil & Gas platforms, Nuclear power plants, electrical grids …)
  → Pierre / Yamada

- IT (ISO/IEC 27000) and JTC 1/IoT (focus on cloud computing)
  → David → in progress

- Smart factory (Industry 4.0) – Link with TC 65 ➔ Link with SEG 7
  → Shawn / Toshi

- Smart Building with integrated systems (link with SEG 9)
  → Shawn / Toshi

- Railways
  → David → in progress

Possible future business applications to be matrix modelled.
- Medical / Healthcare (IEC62304, IEC8001, …)
- Critical Building (Hospitals, data centers, power plants, …)
- Smart Cities
- Connected cars (see JWG11 TC69/TC57 – Cybersecurity for charging car systems)
- SEG 6 : Systems Evaluation Group - Non-conventional Distribution Networks / Microgrids
- SEG 8 : Communication Technologies and Architectures of Electrotechnical Systems

8.2 e-Tech article

Update on January 2018: the article has not been published on e-tech up to now. As this article has now been reviewed, we asked the IEC to publish it.

October 2017: At this meeting WG 17 reviewed and then worked on the e-tech article created by Morand Fachot from the IEC CO Communications department.

See document
CA for cyber_Draft_for_CAB_20171006_Aftermeeting.docx
on the collaboration tools.

This document has been sent to Morand for completion prior to publishing.

8.3 Survey

Update on January 2018: this point has not been mentioned. However, it remains key to get it after the Matrix approach is achieved

See new actions from the February 2017 meeting report.
Extract:

> *In order to have a clearer picture of the market needs, it is proposed to conduct a survey at the national level with the main stakeholders present on these markets and within an international perspective.*

Work to be done on the Matrix Approach (see hereafter, Chapter 8) is a good opportunity to fill in this survey.
It is proposed to work on the Matrix Approach as priority, then, when the results are distributed to the WG17 members (Feb. 2018), to work on the survey at that time.
This survey remains a key element of our WG17 task and, as proposed during the June 2017 meeting, it is tasked to work on the following countries: USA, Canada, Japan, Europe, Russia, China, Korea, Australia and Israel. Results will be provided for June 2018.

8.4 Promotion / Event

It is mentioned that the high number of events or conferences organized around CS represent a huge opportunity to present our knowhow and to promote our schemes.
It is decided to draw a planning of such events and to study the possibility to participate (level has to be checked), including the financial aspect of such a participation. It is also proposed to share this with the IECEE WG on CS.

9 Report to IEC CAB

A written report to CAB will be issued in due time by the convenor before June 2018 meeting, taking into account the development of our works from last October.

10 List of Actions

Who	What	When
Bert	to follow up the proposal made by ERNCIP (see point 6)	Ongoing action
David, Gerhard, Pierre	Make the first proposal of Position Paper – Fast Task Force to work by correspondence	Mid-March 2018
Pierre	Find the EU Contact	Mid-March
Pierre	To propose date for meeting (2nd quarter)	April 2018
Pierre, David	Prepare the work with UNECE	April 2018
See 8.1	Finalize the Matrix Approach	June 2018
David	Ask all IEC CA Schemes to provide their feedback on their needs for CS Certification.	June 2018
David	With a strong collaboration from all WG members, collect information on events related to CS and study a participation of IEC	June 2018
Pierre	Propose to IECEE WG on CS to share the calendar	February 2018.

11 Next meeting

12 June 2018 09:00 – 17:00, Geneva
19 October 2018 13:00 – 17:00, Busan (Korea)

12 Close of the meeting

The meeting ended at 17:00 local time.

ANNEX

Didier Giarratano
Presentation

Context

General

The Cyber Security in Europe today is driven by the **regulation**.

The aim is to protect the critical infrastructures

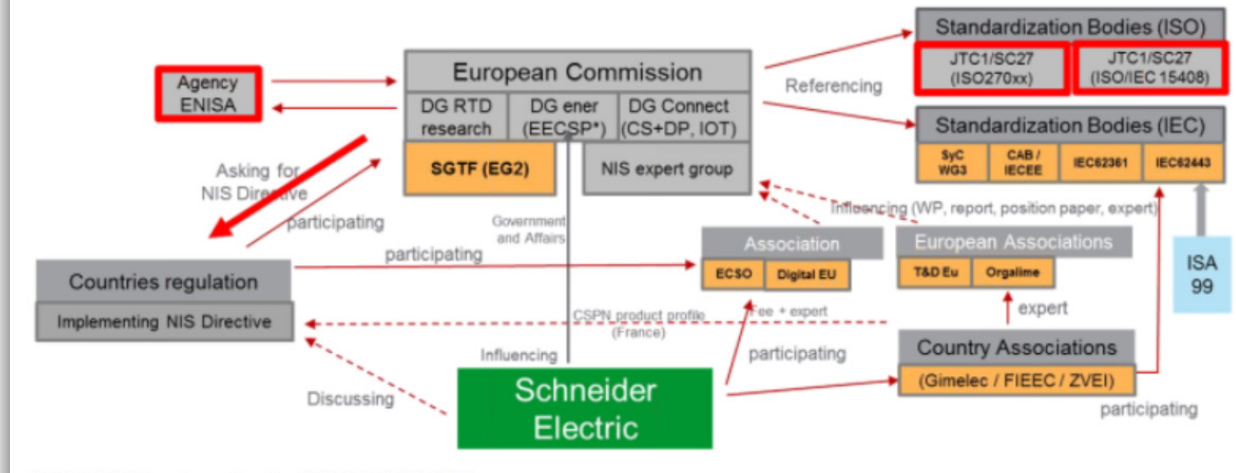
7 domains are impacted;

1. Energy (Electricity, Oil, Gaz),
2. Transport (air, train, water, Road)
3. Banking,
4. Financial market,
5. health,
6. water,
7. Digital infrastructure

The main issue is the certification scheme which is not existing

Life Is On Schneider Electric

Reminder: Cyber Security is Driven by the Regulation
The main Issue for 2018 and onward is the Organization and Product CERTIFICATION



DG = Director General ≈ Ministry

Product certification scheme requirements

As express by some national agencies

- Time Frame (shall be fast)
- European certification scheme
- Done by a Recognized / certified labs
- Done by an Accredited labs by a national authority
- Recognition across Europe (something done in France shall be accepted in a different EU state)
- Several level of security depending on the targeted application / market (self declaration, Level 1, Level 2,…)
- The "pen testing" is bringing values and shall be part of the certification
- And also "sovereign products" (this is pushed underneath)

Life Is On Schneider Electric

Product certification comparison

	CSPN	ISO/IEC15408 Common criteria	IECEE/ CAB IEC 62443	ISA SECURE IEC 62443	UL2900
Time Frame	Available	Available	2/3 years	Available	TBC
European certification scheme	France Only	Yes	YES using IEC scheme	NO	NO
Done by a Recognized / certified labs	Yes	Yes	Yes	Yes	NO (in EU)
Done by an Accredited labs by a national authority	Yes	Yes	Yes(TBC)	No	NO
Recognition across Europe.	France/ Germany/ Netherlands	25 countries	Yes	No	NO
Several level of security depending on the targeted application / market (auto declaration+ Levels depending on profiles)	Based on profile	Based on profile	Based on IEC62443 levels	Based on IEC 62443 levels	NA
The "pen testing" is bringing values and shall be part of the certification	Yes	Yes	No	NO	NA
And also "sovereign products" (this is pushed underneath)	Yes	Yes		NO	NO
Addressing several sectors	Yes	Yes	TBC	NO	YES

IEC15408 is very expensive and can only be applied since the beginning of the design

Self-declaration should be also proposed

Life Is On Schneider Electric

Member	Comments
Gerhard Imgrund	The convenor is kindly requested to provide information about the results achieved by the lobbing at European Level and the further steps that will be undertaken
Rafael Nava	Mexican team believes these activities should be under only one CA System
	Cybersecurity should be promoted internationally, before different countries begin creating individual solutions