	CAB/1849/R
For IEC use only	
	2019-06-19

INTERNATIONAL ELECTROTECHNICAL COMMISSION

CONFORMITY ASSESSMENT BOARD (CAB) **Meeting 45, Geneva, 2019-06-19**

SUBJECT **Agenda item 6.4**

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

Since the Busan CAB meeting, held last October 22, 2018, WG 17 met on March 06 in Singapore.

The report is in three parts:
Part A – Recommendations submitted to the CAB for formal approval
Part B – items of interest to the CAB
Part C – Review of previous CAB Decisions Related to this subject
Annex 1: Minutes of March 2019 WG17 meeting

EXECUTIVE SUMMARY

Several recommendations to the CAB are made in this report after a fruitful meeting in Singapore in March this year.
The key points are as follow :

- *Develop a scheme for the IEC 62351*
- *Strong communication plan involving all the IEC community is requested*
- *Involvement of National Committees is requested to develop the Cybersecurity CA activities globally*

ACTION

Members of CAB are invited to review this report and submit comments, using the CAB commenting system, no later than 2019-05-13, for discussion at the CAB meeting in June 2019.

Part A: recommendations for CAB approval

For more details on each of the subjects here under, it is recommended to read the Minutes of our last WG17 meeting, in Annex #1.

CAB WG17 members have a very high level of concern with the communication around the Cybersecurity CA activities and are motivated to make a proposal. However, this is not part of the WG17 Terms of Reference (ToR) today. Consequently, WG17 is requesting an update of its ToR.

A1. WG17 recommends to CAB to update its Term of Reference, by adding the following sentence at the end :
"When necessary, to make recommendations to the IEC Community for specific communication and promotional actions related to Cybersecurity activities in the field of Conformity Assessment."

National Committees are key resources to deploy and promote our cybersecurity CA activities towards the regulators and to understand local needs to build our Certification Schemes.

A2. WG17 recommends to CAB to request the National Committees, through the National Committees Secretary Forum, to start promotional actions towards their Regulators concerning the IEC cybersecurity CA activities.

Communication material to be used by the different IEC's stakeholders needs to be harmonized, comprehensive and powerful enough to convince regulators to accept our schemes. It is considered that all IEC communities have to be involved to build the communication plan. WG17 concludes that a Task Force should be setup for that purpose, including members from CAB, SMB and communication department.

A3. WG17 recommends to CAB the creation of a Communication Task Force involving SMB, CAB and Comms Department people to build a strong cybersecurity communication plan.

The IEC62351 standard deals with Cybersecurity in the Energy Sector. The standard and the market are now mature enough to develop a new certification scheme in this field. WG17 believes that a Task Force should be setup in the IECEE to develop an operational scheme.

A4. WG17 recommends to the CAB to ask the IECEE to setup a TF to build a new Cybersecurity Certification program aligned with the IEC 62351 requirements.

Following the CAB meeting held in October 2018 in Busan, the IECQ has setup a new WG12 on cybersecurity, dealing with the ISO/IEC 27000 series, to investigate the development of a certification scheme. In order to provide clarification of the role of each IECQ and IECEE in the context of cybersecurity, WG17, recognizing the added value of this new IECQ WG, asks for IECEE recognition of this work and also asks them to monitor this work.

A5. WG17 recommends to CAB to request the IECEE WG31 to recognize and to monitor the work done by IECQ on Cybersecurity.

Part B: items of interest to CAB

The **last WG17 report** from March 2019 meeting is included in **annex#1** for your information.

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

CAB 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.

CAB 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.

CAB 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).

CAB 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.

CAB 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.
  - 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.

CAB 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".

CAB 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.

CAB 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.

CAB 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.

CAB 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.

CAB Decision 43/21 — *Report from CAB WG 17 – Cyber Security*

The CAB thanked the Convenor, Mr Pierre Selva, for the report given in document CAB/1737A/R and urged the group to move quickly toward a situation where it could make recommendations for CAB consideration at its next meeting in Busan.

CAB Decision 43/22 — *European Cybersecurity*

The CAB proposed that the IEC General Secretary coordinate with CENELEC to contact the European Commission and ENISA for a high level meeting on standards and conformity assessment cybersecurity issues at the EU level.

CAB Decision 44/16 — CAB WG 17 – Cyber Security

The CAB thanked the WG 17 Convenor, Mr Pierre Selva, for the document, CAB/1796A/R, and his additional verbal report. CAB was encouraged by the draft UN Common Regulatory Objectives Framework Guidelines for Cybersecurity and gave its endorsement to continue the development with UNECE WP.6. CAB was further encouraged by the news of the high level meeting held between the EU Commission, ENISA, CENELEC and IEC concerning the EU draft Act on cybersecurity and supported ongoing actions in this regard and in other regions of the world.

IEC CAB WG 17 Singapore 20190306
Meeting Report
2019-04-02

IEC Conformity Assessment Board (CAB)

IEC CAB WG 17 2019-03-06 Singapore Cybersecurity

Meeting Date	06 of March, 2019 – 9:00am – 5:00 pm
Meeting Place	Singapore

Present

Pierre Selva	Convenor
David Hanlon	Secretary
Tim Duffy	CAB Member (US)
Ted Gaertner	CAB Alternate (NL)
David Brière	CAB Alternate (CA)
Chris Agius	Ex. Secretary IECEx, IECQ
Toshiyuki Kajiya	CAB Alternate (JP)
Tsutomu Yamada	Hitachi (JP)
Steven Margis	CAB Alternate (US)
Shawn Paulsen	CAB Chair (CA)
Thorsten Arnhold	Guest
Wolfgang Neidzeller	IECEE Chair (DE)
Gerhard Imgrund	Guest
Peter Sieber	Hima
Giovanni Cambronero	ANCE
Marie-Elizabeth D'Ornano	Guest
Ying Wang	SITIIAS
Zhang Aisen	China
Mike Nash	Gamma Secure Systems Ltd
Rudy Belliardi	Schneider Electric
Didier Giarratano	Schneider Electric
Rob Hanson	CSIRO

Excused

Mark Amos	IECEx
Ilan Carmit	The Standards Institution of Israel
David Doggett	Schneider Electric
Kari Hakkarainen	Inspecta
Otto Walch	R. STAHL AG
Alan Sellers	Dyson
Eyal Adar	White Cyber Knight
Kerry McManama	Ex. Secretary IECEE & IECRE
Stefan Rutten	DEKRA Certification

No reply

Wonjun Cho	KTL
Brian Fitzgerald	US Food & Drug Administration
Paul Forney	Schneider Electric
Roland Heidel	Siemens

Shigeyuki Kondo	IECEE Vice-Chair
Valeriy Konyavskiy	Special Bureau of Computer Design Systems
Ken Modeste	Underwriters Laboratories
Siarhei Nazaranka	BELLIS Testing and Certification
Sergei Nazarenko	BELLIS Testing and Certification
Lee Neitzel	Wurldtech
Johan Nye	ExxonMobil
Jeff Potter	Emerson
Andre Ristaino	Automation Standards Compliance Institute
Akio Sato	CSSC
Ragnar Schierholz	ABB

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

Important remark :
all the "recommendations" made in this report are those which will be proposed to the CAB in a separate report.

IEC CAB WG 17 Busan 20181019
Meeting Report
2018-11-14

1 Welcome and Introductions

Meeting is opened at 9:00 am in the Singapore Enterprise facility.
Roundtable to introduce each of us.

2 Approval of Agenda

Agenda is approved with 2 small additions :

- Information about ETSI activities
- Information about activities in IEC CA Systems (IECq, IECEE, IECEx, IECRE)

3 Appoint a secretary for the meeting and note the attendance of the meeting

David Hanlon is appointed as secretary for this meeting.

4 Objectives of the meeting

To make status on regulations
To make proposition to CAB
To make update on last activities (Europe, Marketing, All other countries)
To work on the IEC 62351 program.

5 Remember the term of reference of the 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.
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 Review of last meeting and CAB decision (Busan 10/2018)

The last minute from Busan meeting and the decisions taken at the CAB meeting in October 2018 were reviewed.
From Busan report

- CENELEC TC 65X = IEC TC 65 mirror committee
  - Not all IEC 62443 are available as EN standards, however, an automatic processus exists today to approve the IEC standards as EN standards. The previous blocking points regarding the IEC 62443-2-1 have been unlocked.
  - 62443-2-1 in consistent with EN standards (mostly editorial issues)
  - Issue is between 62443 and a 27000 std

Discussion

- 62443 std as horizontal std
  Recommendation to CAB to propose that SMB redevelop 62443 as horizontal std.
  Maybe need title changes and some terminology changes which are very “industrial automation” oriented/focused.
  Maybe need to take it out of TC 65, or add additional expertise from beyond industrial automation sector.
  Attention is drawn on the risk to loose expertise incase of horizontal standard.

- Need promo/information about 62443 focused at regulators
  Tim and Peter’s comments
  Regulators are mostly at National level, so IEC needs to go through the NCs.
  Need to have a coordination plan with the NCs → maybe NC Sec forum
  Steve comment → regulator promo/lobbying is not in WG 17 ToR. We should ask for an update of our ToR.

  Proposed Process
  Raise Cybersecurity issue at next NC Sec forum.

Propose to create a regulator package
Ask what they need/ can they help create this package
Maybe create a small NC TF
Coordinate with IEC Comms to create the package
Get NCs to translate the package into local languages
Each NC to create a comms program to national regulators

Need an NC cybersecurity "champion" to drive this forward (dedicated promo person ??).

Shanghai GM
Regulator forum → on cybersecurity – As CAB WG, we should be involved in this forum.

Zhang Aisen comment → need material and training to be able to approach regulators

Need to build a strong communication plan around cybersecurity taking into account all the subjects mastered by IEC. Need to have a common group, involving people from SMB, CAB and IEC Comms department.

Recommandation #1. To ask the CAB for an update in our Term of Reference, by adding the following sentence at the end :
"When necessary, to make recommendation to the IEC Community for specific communication and promotional actions related to Cybersecurity activities in the field of Conformity Assessment."

Recommandation #2. To ask the CAB to request the National Committees, thru the National Committees Secretary Forum, to start promotional actions towards the Regulators.

Recommandation #3. To ask the CAB for the creation of a Communication Task Force involving SMB, CAB and Comms Department people to build a strong cybersecurity com plan.

7 European Cybersecurity Certification Scheme proposal

Status on this regulation.
Cybersecurity Act approval is expected Q1or Q2 2019
Now takes standards into account
Risk that cybersecurity aspects will be included in sectoral directives / regulation (LVD, MD, RED, etc)
These directives / regulations are dealt with in separate DGs.
Separate DGs may use different standards or different CA solutions.
So the same products/components, but used in different sectors under different DGs, may be according to different standards or CA requirements. Eg: circuit breaker in medical application or same circuit breaker in electrical utility application may be according to different standards and CA requirements.

Possible Solutions
One horizontal EU Directive (eg EMC Directive)
CS Act CA System will be identically implemented in each sector specific EU directive/Regulation

Didier comment → smart grid recommendation to EU. Report issued by the Smart Grid Task Force - EG2 to EU and ENISA. This report is not officially published now, but you can find a copy here


SGTF_EG2_Report_final.pdf

attached :
This document provides a full map of the objectives in regulation and how to match these objectives with the use of IEC 62443 and ISO/IEC 27002 standards.
It also refers to standards 62443, 62351, 27002
Document also provides profiles for the energy sector.

These profiles should be picked up within IEC TC 65 WG 10 to become IEC profiles → TR (Technical Report).
IECEE could then certify against the specific TRs in its CS cert. services.
(Profiles define a subset of requirements, from defined standards, for products/services used in defined sector applications. When the same product/service is used in a different sector application, a different profile would apply.)
An additional issue is the level of maturity (ML), which may define the level (or depth of) CA required to be done on a product/service against a defined profile. Another approach to this is to have different profiles not only for the sector application, but also for the ML.
Eg: profile 1.1 = App 1 at ML 1. Profile 1.2 = App 1 at ML 2, Profile 3.2 = App 3 at ML 2

Next step : ENISA will wait for the new commission then should start again its work before the end of the 2019 year.

- IEC 62351 – energy sector

Question → where should a WG be established to study a potential CA service.
Reply → probably with IECEE → recommendation to CAB to send a request to IECEE.

Recommandation #4. The working group will recommend to the CAB to ask the IECEE to setup a TF to build a new Cybersecurity Certification program aligned with the IEC 62351 requirement.

- ACSEC Guide 120 → list of standards for CS. The last edition of this guide is date June 2018.
- ETSI releases first globally applicable standard for consumer IOT security : https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security

8 IEC Position Paper

9 Work with UNECE

Status on work progress with UNECE
• UN CRO Guidelines
It was explained that the current document was developed at the initiation of IEC, but in collaboration with UNECE. The base concepts in the document were approved at the UNECE November 2018 meetings, but it was also recognized that the document was not complete and needed additional work.

Currently work is being done to add GMM examples for AAL, automotive, railways, energy utilities, smart grid, medical & health services and organizational CS.

The UNECE WP.6 GRM (risk management group) is also working to add content on the risk analysis aspects of the methodology.

Next actions are to submit the updated document to UNECE by end July for translation into 6 languages and distribution to all UN members for comments and feedback ready for discussion and approval at the November 2019 UNECE WP.6 meetings in Geneva.

Attention is drawn on the use of the IEC logo / name in the document. We need to be sure to avoid any confusion and the feeling that this document is the IEC position. It should be mentioned only that the IEC was contributing to this document.

10 Communication activities

- Promotion - certainly of new activities
  IECEE has issues with strict specification of budget allocations and a “long” process to gain approval for deviations from specifications but still within the subject of the budget item.
  IECQ and IECEx have greater flexibility in this regard with the Executive having the authority to take decisions on promotional activities so long as the costs remain within the bounds of the budget allocation.

  Need a recommendation to CAB that CA System budget allocations for promotion be increased and that flexible process are created to allow fast spending decisions.

  On the other hand, promotional planning should be better managed, with speaker events known and scheduled well in advance (eg: Cyber Senate events).

  The WG17 recognizes that there are multiple opportunities to promote cybersecurity activities and is asking the CAB and the IECEE to make proposals.
  As mentioned in the chapter 6, recommendation #3 of this document, WG17 encourages the cration of a strong communication plan involving all the active parties of IEC.

11 IEC 62351 : Power Systems Management and Associated Information Exchange – Data and Communications Security

Introduction to the standard and identification of main needs.
Prepare communication to the CAB
See chapter 7 of this document for more information.

12 Matrix approach

No work done on this subject during this session.

13 Activities in other CA systems and sectors

- IECEx perspective of CS
  Watching brief.
  It is considered that specific CS services for Ex are not needed yet.

- IECQ perspective of CS
  Received requests from CBs to add scope for CS certification of QMS.
  WG12 formed to discuss this issue.
  If goes ahead likely to 27001.
  Cert. to 27001 is already largely done in the world, but with significant variation between CA results, therefore mutual recognition difficultly.
  It is believed IECQ would bring more consistent results and therefore allow for mutual recognition.
  Recommendation to CAB to have IECEE recognizes and monitors the work on CS in IECQ.

Recommandation #5. The WG17 ask the CAB to request the IECEE WG31 to recognize and to monitor the work done by IECq on Cybersecurity.

- IECRE perspective of CS
  No request for now.

- Mexico perspective of CS
  It’s moving slowly, but no huge work on progress at regulatory level

- Canada perspective of CS
  Nothing special to mention. The IEC62443 has been adopted by CSA. No news on regulation

- USA perspective of CS
  A new regulation has been setup in California and it should be followed by 5 or 6 States. There is a push to use International standards. ISA Secure and IEEE have been approached. NEMA is asking for more harmonization of the applicable rules – Need to have a federal regulation ?

- Japan perspective of CS
  More or less confuse situation !
  The Telecom Business Law is asking for device providing protection against attack, but nothing explains how to do it.
  Penetration tests are deployed by communication ministry on consumer products.

- UK perspective of CS
  Here also the situation is confused, mainly due to Brexit issues.
  2 options are on the table : Continue t stick with European Rules, or, Build a completely new system.
  But UK wants to remain in the CEN/CENELEC and to use these standards.
  The top priority are the Consumer IoT devices.

- Australia perspective of CS
  The biggest concern is about the data protection and privacy. This is based on national standards, themselves based on ISO/IEC 27000 series.

- Marine sector perspective of CS
  The use of industrial standards seems to be the trend.

- Germany perspective of CS
  For critical infrastructure, the ISO/IEC 27000 series will be the preferred one.

- Household appliances perspective of CS
  - 60335-1 deals with the safety of electrical appliances for household and similar purposes
  - Remote communications through public networks shall not impair compliance with this standard. See annex XY.
  - Appliances intended for remote communication through public networks.
  - In general it does not cover aspects concerning confidentiality of data and consumer privacy.
  - (In general it concerns only issues of risk to safety caused by external communication.)

14 Location and Timing of the next IEC CAB/WG 17 Meeting on Cyber Security.

Opportunity : Shanghai /Oct 2019
Any other proposal ?

15 Close of the meeting