For IEC use only	**CAB/1626/R** **2017-04-20**

INTERNATIONAL ELECTROTECHNICAL COMMISSION

CONFORMITY ASSESSMENT BOARD (CAB) **Meeting 41, Geneva, 2017-06-13**

SUBJECT **Agenda item 6.10**

Report from CAB WG 17 - *Cyber Security*

TERMS OF REFERENCE

Under CAB Decision 35/8 WG 17 was established with the original terms of reference (ToR) being to investigate the market needs for possible CA services in Cyber Security. The ToR were modified slightly in CAB Decision 36/13 taken in Tokyo, and again in Decision 37/21 taken in Geneva 2015.

The current ToR given below reflects two decisions 39/01 (by correspondence) and 39/23.

CAB WG 17 scope is as follows:

- 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 document follows on from the previous report, CAB/1565/R, which was submitted to the October 2016 CAB meeting.

From the last CAB meeting, up to now, 2 CAB WG17 meetings have been hold. One by remote mode on November 28, 2016 and the second one during a full day in lake Forest (USA) on February 08, 2017.

This document is a brief update of the current status of the work of WG 17.
This report includes an executive summary of progress since the last report.

Part A – Recommendations submitted to the CAB for formal approval
Part B – Other items of interest
Part C – Review of Previous CAB Decisions Related to this subject

EXECUTIVE SUMMARY

The Cybersecurity Conformity Assessment is a very complex world with a multiplication of actors and organizations.

Several initiatives are taken around the world by different organizations at national, regional or sectoral levels.

The need for Conformity Assessment and/or Certification schemes is confirmed by stakeholders.
Main IEC inputs are coming from JTC1 and ACSEC.

e-Tech article will be issued after the approval of the new IEC62443 program launch by the IECEE.
A survey will be conducted at national level to better understand the stakeholder needs.
Monitoring of several initiatives and organization has been shared between WG17 members.
Useful links to organizations has been provided to WG17 members.

Part A: recommendations for approval

At this stage, no recommendations for approval are requested by the working group.
The WG17 should be ready to make first recommendations during the next CAB Meeting in October 2017.

Part B: other items of interest

The minutes of the last meeting held in Lake Forest (USA) in February 2017 is attached as Annex #1 for information.
It has to be noted that a survey is ongoing at national levels by several members of WG17 and that the first results will be discussed during our next half day meeting which will be held on June 14 in Geneva.

Part C: Review of Previous CAB Decisions Related to (WG or Other)

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.

ANNEX #1 – 2017 Lake Forest meeting Minutes

CAB WG 17 Lake Forest 20170208
Meeting notes
2017-02-10

IEC Conformity Assessment Board (CAB)

CAB WG 17 2017-02-09 Lake Forest Meeting Notes
Cybersecurity

Meeting Date	8th of February, 2017
Meeting Place	Intertek Testing Services NA, Inc. 25800 Commercentre Drive Lake Forest, CA 92630 USA

Present

Gaertner, Ted
Hanlon, David
Kajiya, Toshiyuki
Margis, Steven
McManama, Kerry
Neitzel, Lee
Rutten, Stefan
Selva, Pierre
Yamada, Tsutomu
Amos Mark

On Remote

Adar, Eyal
Forney, Paul W.
Giarratano, Didier
Nash, Michael John

Some Abbreviations

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

1 Opening of meeting

Opening by the convenor at 09:00.
Welcome to new members and apologies
Approval of the agenda (on Collaborative tool).

2 Review of last meeting minutes

Review of the last remote meeting held on November 28, 2016.
See document available in the Collaborative tool.
Few comment have been received after the meeting and are integrated in these minutes.

3 Presentations

Presentations or updates were received as follows:

➔ Lee Neitzel – IECEE TF – Summary of ongoing work

Progress was made during the IECEE TF meeting on Monday 6th and Tuesday 7th of this week (the two day prior to this meeting).
- OD 2037 Model for CS Certificate
- TRF updated for 62443-2-4

If the draft documents are approved by the IECEE CMC in May, then a workshop/training session is(are) planned for August.
- Training for lab managers (half day) - 62443-2-4
- Training for lab evaluators (few days) - 62443-2-4

➔ Mike Nash – ACSEC update by remote
(see *ACSEC Presentation Nash.ppt* on Collaborative tool).

ACSEC first created a listing of standards from IEC and other SDO containing security requirements. Then a database (DB) of IEC standards was created from this listing. The DB contains information on the TC/SC that developed the standards, the publication name and title, the level of abstraction, the target users/audience, the application domain and a link to the standard in the IEC webstore. Not all of this information is filled-out yet for all the listed standards.

ACSEC has completed the first draft of a guidance document for standards writers titled:
IEC Guide for implementation of Information Security and Data Privacy in IEC Standards
This document was submitted to IEC NCs for comments.
The comment are planned to be resolved at the next ACSEC meeting on March 20th in Paris.
This first draft is available on the Collaborative tool as *AC_20172e_AC.pdf*.
The guide (which may become Guide 120) has a structure as follows:
- Guidance on terminology → recommended and other sources
- Categorisation of security standards → types of standards, relationships, content
- Existing IEC security standards → link to ACSEC DB
- Considerations of security standards development → cookbook
- Conformity assessment advice in sections 5.6.4 and 7.4.1

Comments have been addressed concerning the difference between glossary in this guide and some other glossaries in, for example, standards such as the ISO27000 series or the IEC99 guide.

This issue has to be carefully understood by the evaluator when they will have to make analysis and assess conformity of products, service or processes.

➔ Eyal Adar – Europe update by remote
(see *WCK Portal_ customers 2016 v8.docx* on Collaborative tool).

EU Commission strategy
- Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats
- The Commission will look into a possible European certification framework for ICT security products.
- **NIS Directive** on network and information systems has been published (July 2016)
- From August 2016, Member States will have 21 months to transpose the NIS Directive into their national laws and 6 months more to identify operators of essential services.
- Businesses in these sectors that are identified by the Member States as operators of essential services will have to take appropriate security measures

- MSP – European Multi Stakeholder Platform – since 2011 – specifically for ICT

- Focus Group on Cybersecurity (CSCG) has been established in 2016 at the European Level (CEN-CENELEC-ETSI) to provide strategic advice on standardization in the field of IT security, Network and Information Security (NIS) and Cyber Security (CS).

- Both of these groups (MSP and CSCG) liaise with the ENISA.

ENISA (European Union Agency for Network and Information Security)
https://www.enisa.europa.eu/
- Helps the Commission, Member States and the business community to address, respond and especially to prevent NIS problems.
- Collaborated with CEN, CENELEC and ETSI
- Key studies - Survey of Risk Management Methods, Frameworks and Capability Maturity Models for the EU Network Information Security Platform (published on ENISA web site in early 2015).
- Results of public consultation (July 2016)…
    - The majority of respondents stressed the importance of cybersecurity certification schemes
    - many (37.9%) thought the current certification schemes did not support the needs of Europe's
    - A large share of respondents (50.4%) stated that they did not know whether certification schemes were mutually recognized. Among those who answered more than half felt the current certification schemes are not widely recognised across the EU.

IEC is not visible within these activities.
(Maybe need a coordinated outreach by CAB WG 17 & ACSEC.)
Most of the people participating to ENISA work are coming from IT Industry.

62443 series (certainly -2-1) originally blocked by CENELEC as an EU standard
Certain blockings are reviewed each year.
(EU policy is EU standards first, IS only second.)

Need to know the current status of acceptance of the various 62443 standards as EU adoptions.

➔ Tsutomu Yamada – Japan update
(see *170208_SecurityActivity-Japan-r1a.pdf* on Collaborative tool).

Main CS concerns in Japan
- IOT
- Critical Infrastructure - 13 sections, including
  - Electrical power supply – smart grid, control systems, etc
  - Railways
  - Gas supply
  - etc

Solutions are being driven by
- Industrial standard activity
  - IEC JNC members discussing security concepts and requirements for Industrial Control Systems and CI systems
  - Total Concept for Manufacturing system security – adaptive, responsive and cooperative system to withstand new threats in the connected systems.
- Government oriented activity
  - There have been 4 action plans since 2000

CS certification activities in Japan
- ISASecure (ISCI)
  - EDSA (Embedded Device Security Assurance)
  - SDLA (Security Development Lifecycle Assurance)
  - 1 Japanese laboratory certifies to ISASecure (Control System Security Centre – CSSC)
- Achilles Communication Certification (Wurldtech)
- CSMS (Cyber Security Management System)
  - Certified by JIPDEC based on IEC 62443-2-1
- J-CLICS (Check List for Industrial Control System)
  - Check lists to help identify and understand security issues https://www.jpcert.or.jp/english/cs/jclics.html

➔ Shawn Paulsen – Canada Verbal update
(see *CAB WG 17 Canadian Update.docx* on Collaborative tool).

- Canada is very active in JTC-1
  - ISO/IEC 27XXX series
- Public Safety Canada is supporting IEC 62443 for security for critical infrastructures.
- Canada is looking to develop technologies to better protect their cyber infrastructure.
- Canadian Institute for Cybersecurity established
  - Research and training focused on industry and public sector needs and to identify and develop solutions for cybersecurity initiatives for industry, healthcare, and interconnected products, risk analysis, and testing.
  - Current research into critical infrastructure protection, Security Analysis and Risk Management, Intrusion Detection and Prevention.
- There is interest in developing a program for service offerings related to cybersecurity.
  - Will cover connected products (IoT), Smart Homes, Industrial Control and Healthcare
  - Gap Analysis and Risk Assessment Service – evaluation of Information Security Management System and Security Development Lifecycle.
  - Vulnerability Identification Testing
  - Penetration Testing
  - Communication Robustness Testing – to ISA Secure EDSA specifications. We currently cannot issue certificates to this as there is no licence agreement in place at this time.

- Reviewing potential evaluations to IEC 62443 series using ISA Secure Scheme.
- Assessments can also be performed to UL-2900 and NIST 800 frameworks; 2900-1 General Requirements, 2900-2-1 Network connectable components of Healthcare Systems, 2900-2-2 Industrial Control Systems.

➔ Didier Giarratano – French verbal update by remote

The French regulator has issued a regulation in 2014 called LPM (Loi De Programmation Militaire)
Under this regulation it is mandatory for all of the critical French organizations to setup a cyber security program in order to be able to manage the potential attacks.
The critical organizations include: the army, government, hospitals, information, telecommunication, energy, etc.
The French Security Agency (ANSSI) has issued some guidelines based on a risk assessment on how to protect a critical infrastructure.
In addition, they have created a certificate that can be applied to products.
This certificate is called CSPN (Certificat de sécurité de premier niveau) and has been created to avoid needing to pass common criteria certification which doesn't make so much sense for an industrial product.
To get this certificate you need to define a cyber Security profile for your product with the ANSSI (eg: today an official profile is available for the PLC)
The test is 3 weeks of penetration testing based on the profile.

Industrial IOT Security Consortium - www.iiconsortium.org/
Document: Industrial IOT Volume G4 : Security Framework
http://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf
IECEE mentioned on page 130.

4 Update on action list following last meeting

➔ Etech Article

It had been found that most industry/market sectors could not articulate their cybersecurity (CS) needs, but when presented with a set of potential solutions/services, they quickly agreed that those were what they needed. So the original goal of this article was to make various industry/market sectors aware of the IEC's CA initiatives with regard to CS and invite them to participate.

For various reasons and although 3 attempts were made, the article was never written as required and therefore never published.

At this meeting it was again decided that an article was necessary, but that it should be written on two levels; one directed at the general public, and a section (box section) written at a deeper technical level. As a conclusion it should ask the question "why can't these proposed services be used in your sector" and invite the readers to respond to that.

Additionally a "white paper" on the IECEE CS programme should be created and available as a linked document to the etech article.

It was also agreed that this article should be published after the IECEE CMC meeting, in May, and that if the CMC approves the IECEE TF on CS programme, the subsequent workshop/training (possibility to be held in August) should be mentioned in the article.

Once the article is published the IEC Technical Officers, TC/SC Chairs and Secretaries form the ASCEC DB of standards should be individually informed and requested to share this articles with their members and to encourage them to provide answer to the open questions.

Editorial team will have to write this article.

5 New actions – How to obtain quick win ?

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.
For that purpose, it is suggested to use the survey guide presented here in annex#1.

This survey is intended to answer the questions here after.
As an introduction, we could use the IEC62443-4-1 presentation sent by Lee Neitzel and the one made by Eyal in October 2015 available as attached files here :


IEC 62443-4-1 Overview.pdf


IEC 62443 for Energy V2.pdf

Ideally, this survey should be made before our next CAB meeting in June in order to give an overview to the CAB members.
All members of our WG17 should conduct this survey in their own country.
It is requested to inform the WG17 secretary and the convenor if you expect to conduct this survey.

5.1 Is the IEC62443 series of standards applicable to domain outside of its original scope ?

View from Manufacturers
View from Certification Bodies
View from Service providers
View from Regulatory bodies

5.2 In which sectors do we need to investigate (need small teams to provide argued answers)

Smart Grid
Smart Building
Railways (2nd Annual Rail Cyber Security Summit – London – 14&15 March)
Connected cars
IT Business
Medical / Healthcare

Mass product (IoT – Connected consumer products)
Critical products (Used in critical infrastructures)

Any other sector ?

5.3 Links with external bodies

The CAB Secretariat will check to what extent official liaisons can be established with these organisations taking into account IEC National Committee concerns and requirements.

At this stage the persons named are asked simply to monitor the discussions, developments and actions of the organizations and to report key elements of interest to CAB WG 17.

- UNECE - www.unece.org/trade/wp6/welcome.html — CAB Sec.
- ENISA - www.enisa.europa.eu — Eyal Adar
- WIB - www.wib.nl — Stefan Rutten
- ENCS — Stefan Rutten
- ISA Secure - www.isasecure.org/ — Paul Forney
- National or Regional Security Agencies (like ANSSI in France) — Every member
- National or regional authorities — Every member
- SOGIS MRA (IT) – www.sogis.org
- ECSO (European Cyber Security Organization) – www.ecs-org.eu
- CSCG (Focus Group on Cybersec.) - https://www.cencenelec.eu/standards/sectors/defencesecurityprivacy/security/pages/cybersecurity.aspx

New, not discussed in the meeting.

- T&D Europe - www.tdeurope.eu/en/home/
  Interesting doc: http://www.tdeurope.eu/data/TD%20Europe%20-%20Position%20Cyber%20Security_291116.pdf
- Online Trust Alliance - www.otalliance.org
- Digital Europe - www.digitaleurope.org/
- Industrial IOT Security Consortium - www.iiconsortium.org/

➔ Liaison with internal bodies

- ACSEC — Ken Modeste

6 Next meeting

Depending on the results for survey mentioned in chapter 5, a possible half day meeting in Geneva in June in the CAB meeting week.

The meeting ended at about 17:00.

ANNEX # 1

Guide to conduct survey at National Level within an international perspective

Basic information

Country
Date
Interviewer (Name and organization)

Interviewee

Name

Organization

Category of activity

Example :
Manufacturer
Authority
Regulatory body
Service provider
Professional association
Certification body
Other : _____

Sector of activity

Example :
Smart Grid
Smart Building
Railways (2nd Annual Rail Cyber Security Summit – London – 14&15 March)
Connected cars
IT Business
Medical / Healthcare
Mass product (IoT – Connected consumer products)
Critical products (Used in critical infrastructures)
Other : _____

Scope of activity (National, regional, international)

Introduction of the subject

Cybersecurity is clearly recognized as a subject of high interest by all stakeholders
Cybersecurity certification as a limited scope today
Most of the consortia / fora are developing, or would like to develop, program(s) for certification.
IEC proposes a new program for Industrial Automation program based on the IEC 62443-2-4 standard and is developing a program for the IEC 62443-4-1
Purpose of this survey is to identify the needs in your specific area, and to check to which extend the use of the IEC62443 series could help to answer these needs.

Understanding the interviewee needs

What is the picture of their sector needs ?

Standards, organizations and main actors, market relevance, market drivers, identified gaps, key points, timeframe, hardware, software, systems, process, personal, …

Do they have clear needs in term of cybersecurity certification ?

If yes,
How do they manage their certification ?
Which standards do they use ?
Which certification body(ies) do they use ?

If no,
Do they believe certification could help them to make business ?
What could be the ideal framework to get these certification (independence, recognition, easy to use and to understand, ….)
How the IEC could help to develop a certification framework ?

Are they involved in external organizations dealing with Cybersecurity certification ?

If yes,
What are they doing in these organizations ?
Can they describe the ongoing work ?
What would be their interest to have a close link with IEC Conformity Assessment schemes to develop their certification program ?

Are they ready to invest time with other stakeholders to develop a cybersecurity certification framework ?

Eg: Participation in national or international working group(s).

Main conclusions

Needs are identified Yes / No
Standards are known Yes / No
IEC 62443 could be used Yes / No / Don't know
Timeframe need < 1 year / 2-3 years / More / Don't know
IEC CA System could be the right framework Yes / No
Ready to participate IEC CA System work Yes / No
Other organizations have been mentioned as competitor Yes / No
If so, which one(s) ?