For IEC use only

CAB/1504A/R

2016-05-17

INTERNATIONAL ELECTROTECHNICAL COMMISSION

CONFORMITY ASSESSMENT BOARD (CAB) **Meeting 39, Geneva, 2016-06-13**

SUBJECT **Agenda item 6.6**

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, decided in a vote by correspondence in December 2015, are as follows:

Decision 39/02 — *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.

BACKGROUND

This document replaces the original, CAB/1504/R, circulated 2016-04-18. The only change is in the Terms of Reference box above. "Decision 39/022" has been corrected to read Decision 39/02.

CAB WG 17 was established under CAB Decision 35/8 in June 2014 (see Part C of this document).

WG 17 has held meetings in London in August 2014, in Lake Forest in February 2015 and in Frankfurt on October 2015 and a web conference in December 2015, and has submitted the following reports, CAB/1316/R, CAB/1383/R, CAB/1417/R.

CAB Decision 39/02 (see Part C of this document) was taken by correspondence in December 2015 modifying the scope of the working group (see section on ToR just above).

This report includes an executive summary of progress since the last report.

Part A – Recommendations submitted to the CAB for formal approval
Part B – Main body of the report
Part C – Review of Previous CAB Decisions Related to (WG or Other)

Appendix A – (Supporting Materials for Topic from Report)

EXECUTIVE SUMMARY

The previous report CAB/1417/R, listed 6 actions as the next steps for WG 17 (see Part B of this document).

Three of these 6 actions have been completed. Another action concerning the development of an e-tech article is under way (but not completed at the time of writing this report). Another action which depends on feedback from the published e-tech article has, of course, not yet been commenced. One remaining action concerning reinitiating discussions with WIB has not progressed.

Some discussions were held between the WG 17 interim convener and representatives of RSSB (UK Rail Safety and Standards Board), concerning cyber security.

Ongoing information from ACSEC was collected.

Part A: recommendations for approval

In report CAB/1417/R, dated 2015-11-19 (just after the CAB meeting in Minsk) the Executive Summary had the following note from the CAB Chair:

CAB Chairman's Note: The CAB Chairman regrets the sad news of the death of Mr Ron Collis, the Convenor of this working group. In this situation, as a practical measure, the CAB Chairman names the CAB Secretary, Mr David Hanlon, as the interim Convener of WG 17.

A.1 It is recommended that a new permanent convener for this working group be named.

In report CAB/1417/R, there was also an action item as follows:
Action: Formalise CAB approval of Ken Modeste as liaison to ACSEC and review any feedback from that liaison with emphasis on the 600 odd Standards that ACSEC is reviewing for Cyber Security content and the TC's involved.

A.2 It is recommended that Ken Modeste be formally named as CAB WG 17 liaison to ACSEC.

Part B: main body of the report

Since the previous written report, CAB/1417/R, in November 2015, WG 17 work has been focused on the next steps that were indicated in that report, as follows (numbered here for easier identification):

Action (1): Since the ad hoc group has been dissolved, all former members shall send any reports or market information for Cyber Security they have to the WG 17 Convener, if they haven't already done so.

Action (2): E-tech article on the work of CAB WG 17 and the current work program in IECEE PSC WG 3 concerning cyber security and how it can be applied generically to many sectors. (drafting team – Shawn Paulsen, Eyal Adar, Lee Neitzel, Steve Margis, Tim Duffy, David Hanlon)
David Hanlon – liaison with E-tech team.

Action (3): To review any feedback that may result from the E-tech article

Action (4): Formalise CAB approval of Ken Modeste as liaison to ACSEC .and review any feedback from that liaison with emphasis on the 600 odd Standards that ACSEC is reviewing for Cyber Security content and the TC's involved.

Action (5): Upload the ACSEC minutes and standards list to the WG 17 collaborations tools site. ACSEC → liaison CAB → report from September 24th meeting

Action (6): Re-initiate discussions with WIB.

Actions (1) and (5) have been completed.
Action (4) will be completed at the June 2016 CAB meeting.

For Action (2), a web conference was held in November by the drafting team and two members of the e-tech team, Morand Fachot and Claire Marchand. Draft text by Tim Duffy was shared with the drafting team. It was decided that this draft text would form the basis for a generic (multi sectorial) article about cyber security with the current intentions of the IEC CA activities on this subject (specifically the current actions of IECEE PSC WG 3) to be included. It was decided that other members of the drafting team would make contributions to the base text (which was done over the few following weeks) and then the consolidated version would be handed to Morand Fachot to add some "world content" and modify the text into an e-tech article. Morand Fachot had been following articles on cyber security in the international press for some time, and had accumulated a number of examples.

The next step would be to publish this article in e-tech, then to create a few more sector specific versions, and publish those in sector focused magazines and journals. Both the e-tech article and the sector specific versions would try to solicited feedback from their respective audiences. Action (3) speaks to this feedback.

Morand has completed a general article on cyber security but as yet his article and the drafting group text have not yet been integrated. So at the time of writing this report, the e-tech article is not yet complete, therefore the sector specific articles are not yet complete and action (3) has, of course, not been started. It is hoped that the e-tech article will be completed before the June CAB meeting, where a verbal update can be provided.

Generic model

In February discussions were held between some WG 17 members, by an exchange of emails, in an attempt to develop a generic model in graphical form for cyber security conformity assessment. As consensus was not reached, this will be an ongoing pursuit.

RSSB

The WG 17 interim convener was able to open a dialogue with representatives of the UK RSSB (Rail Safety and Standards Board). The interim convener was able to benefit from his presence in a meeting at RSSB (concerning unrelated IEC worked) to establish contact with Maria Grazia, the person delegated as being responsible for the cyber security initiatives at RSSB. The RSSB's work on cyber security is governed by their 2012 strategic document named, The Future Railway, which provides a vision of the UK railway system out to 2040. Appendix A provides a link to this document and some others. The RSSB is interested in the IEC's work on conformity assessment for cyber security and further discussions are anticipated.

ACSEC

At its meeting in October 2015, ACSEC set itself two principle tasks, firstly to develop a guidance document for standards writers and secondly to continue the mapping of standards with cyber security elements into sectorial and application categories. For the purposes of WG 17's work, the second task is of greater utility. Unfortunately for WG 17, ACSEC decided to give priority to the first task. As a result, a draft guidance document is being developed and a first uncompleted draft has been produced for their next meeting that will take place in Milan in on May 17th.

In an early review of standards having cyber security elements ACSEC created a list with more than 650 standards. These standards were essentially from international SDOs, but did also include some regional and national SDOs such as CEN, CENELEC, ETSI, ANSI, BSI, BUND, etc. IEC's contribution to that initial list was about 100 standards. A subsequent review revealed that many of the IEC standards indicated were actually standard series and that the true number of individual IEC standards was closer to 400. ACSEC have since created a "cleaned-up" version of the list of standards now including only IEC and JTC1 standards, with almost 200 standards in total.

If we consider that a modern system essentially consists of

- interacting, interrelated, or interdependent components forming a user value entity and
- that the components can be confined to a limited physical location, or spread out over a large physical distribution and
- that some degree of human interaction is required for the system's design, realization, operation, and/or use, and
- that the components and their interconnections need periodically to be repaired, replaced, updated or upgraded and
- that many of those components transmit and receive information between themselves and beyond the system itself and
- that they are, or could be, susceptible to possible events, whether internally or via some external public connection, that alter the system's ability to operate as intended,

then the needs for cybersecurity protection of systems become pretty generic.

In summary, the systems that concern us for the issue of cyber security are made up of

- components (which can be physical or virtual),
- interconnections (the systems integration),
- information flows, and
- interventions (human, virtual or automatic).

To ensure best cyber security coverage for a system as a whole, best practices need to be applied for each of these elements and the system holistically. The way to evaluate and validate the application of best practices is through the assessment of the conformity to those best practices.

If, generically speaking, different systems have so many commonalities, it then becomes rather obvious that there must be considerable overlap and redundancy in the almost 200 IEC and JTC1 standards (and more than 650 standards from the initial list).

If a global CA scheme or system is requested by the market with the objective to provide CA services to the widest range of sectors, then it is also rather obvious that the number of standards will need to be drastically reduced, or that some form of equivalence between standards from different sectors will need to be accepted.

We hope that, at least within the context to the IEC, this issue will be considered as a horizontal issue and that some guidance and instruction will be given to the TC/SCs to eliminate their redundant individual sector cyber security requirements and, rather, refer to a limited number of core standards covering their needs.

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 39/02 — 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.

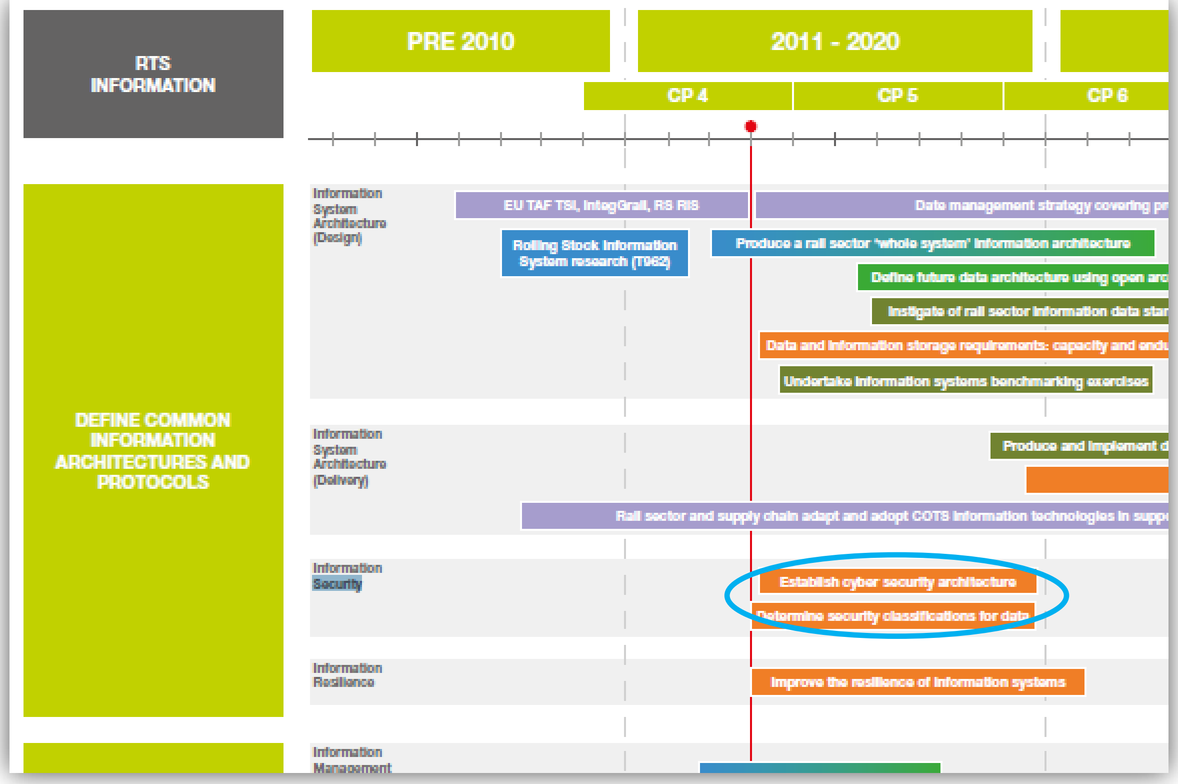
Appendix A:

Source RSSB:

The Future Railway
The industry's rail technical strategy 2012
Supporting railway business

http://www.rssb.co.uk/Library/Future%20Railway/innovation-in-rail-rail-technical-strategy-2012.pdf

Section of page 56.



Other RSSB Cyber security links

http://www.rssb.co.uk/improving-industry-performance/cyber-security

http://www.rssb.co.uk/Library/improving-industry-performance/2016-02-cyber-security-rail-cyber-security-guidance-to-industry.pdf

http://www.rssb.co.uk/Library/about-rssb/2014-05-08-board-paper-B2-Cyber-Security.pdf

https://www.cesg.gov.uk/scheme/certified-cyber-consultancy