Webinar of 2022-02-08

Workshop ''Security in the cyber-physical space'

Questions & Answers

1	As nowadays we are doing some online training for cabin crew, what extra measures can we take to protect sensible data?	- Training staff to the human dimension of cybersecurity and making them aware of the insider threat. - Enforcing a security culture within the company.
2	Further to the liability issues, how can standardization help in gathering consistent physical and cyber evidence and logs to conduct investigations after a cyber physical attack?	The IEC 62443 series includes requirements on technical specification of the logs (what to log etc.) and on security of the logs (e.g., to prevent or detect that the audit trail/logging function is turned off by an adversary). The series also includes requirements on organization measures/procedures to ensure service provider has the capabilities to cyber security incidents including logging and reporting. Standards help by specifying requirements on what needs to be done to ensure that it is possible to consistently record evidence, securely store evidence that can be used by investigations.
3	There is much talk about using a risk-based approach, which I believe is right and better than a compliance-based approach. However, we need to define what level of risk is acceptable. This is a hard question to answer. How are we going to specify acceptable risk? Who decides?	This should come out of the risk assessment: every company needs to define for itself its risk "appetite" and what level they are ready to accept. Companies may wish to contact their national authorities for advice.
4	You should put the links to the toolkit to the chat for accessing it.	Here's the link to the cybersecurity toolkit mentioned: https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_en
5	Presenters have described very clearly the need for integration between cyber security & physical security, IT & OT. I would add another: cyber security & safety. Of all the integration challenges, I believe this one is the most challenging and, for cyber-physical systems, a vital one. I do not hear this being	There may be safety implications to cyber and physical attacks. Safety and security are usually addressed differently, in some cases because they were introduced according to different timings. For example, in aviation while safety is part of the DNA, security measures have been introduced later and progressively, and driven by

	mentioned. Can you comment on this relationship and how you are addressing it?	attacks. Moreover, among other things, the relevant authorities and the handling of information related to safety and security are different. Therefore, safety and security have been traditionally handled separately. It would call for another debate.
6	Is there a more detailed EU level guidance on implementation of cyber security requirements in aviation besides the Toolkit? European version of Doc8973?	DG MOVE has prepared an Information Note on the implementation of cybersecurity requirements under Regulation 2015/1998 and another on critical ICT systems. These can be obtained through national authorities on a strictly need to know basis.
7	Is exists some link between utility devices under MID/2014/32/EU and IEC 62443?	As the MID/2014/32/EU is outside scope of CLC/TC65X, we are unable to answer this question.
8	The use of Eurocae ED-205 in aviation as a support - still valid and useful?	We cannot comment on the relevance of non-CEN/CENELEC or ISO/IEC standards.
9	Does the IEC 62443 cover RED 3.3 CSA and the AI directive?	Regarding the CSA: As a result of the JRC ERNCIP project, there is a proposal for the ICCS certification scheme based on IEC 62443-4-2 and IEC 62443-4-2. Regarding the RED 3(3)(d/e/f) CS delegated acts, there is work in progress ongoing by the ESOs.
10	Don't we face a rising combination of physical and cyberattacks which means that approach need to be holistic...	Absolutely. It is the only way to address it: by creating multi-disciplinary teams, project-based, looking at the risks, and addressing them together.
11	What is the time schedule of new Machinery Directive revision?	Since this Directive is the responsibility of another Commission service, we are not in a position to provide an answer. We suggest that you get in touch with our colleagues in DG GROW
12	Is there any plans to harmonize any parts of EN-IEC 62443?	At this point in time, we are not aware of any proposals on the table for this.
13	When it will be released a new version of 62443? Will it be fit for the framework using it? (e.g., the NIST?)	The NIST CSF has mapping tables in it for IEC 62443. We expect that the future versions of the

		NIST CSF will update the mapping tables as additional parts of the series are updated. Each part of the series that is under revision/or is a new version of the standard has project in the IEC with dates for publications. The current version of the Road map points to a consistent set of documents in place by 2027. We hope the market requirements will bring this forward in time.
14	And to what extent will next revision of Machinery Directive reference IEC 62443-x when incorporating Cyber security	Since this Directive is the responsibility of another Commission service, we are not in a position to provide an answer. We suggest that you get in touch with our colleagues in DG GROW
15	... so challenge between IT Dept. and Security Dept. ...	It is a challenge but also a necessity to have IT and security departments work together in order to address the cyber-physical security.
16	It is not clear how IEC 62443 series can cover IoT devices such as thermostat or others?	Work is ongoing regarding application of the IEC 62443 standards to the Industrial Internet of Things. A thermostat or other measurement product such as a vibration sensor is an example of an embedded component. For such devices, the IEC 62443-4-1 (secure development lifecycle) and IEC 62443-4-2 (security requirements for components) standards apply.
17	How does the implementation of a Enterprise Security Risk Management (ESRM) as a strategic security-program management approach fit into the scheme? Have you considered using the published guidelines for ESRM which have been issued by ASIS International as a possible basic common ground?	Answer from CoESS: not so far, and thanks for the suggestion.
18	Any plans by the Commission Services to Harmonise std 62443 under revised LVD, EMCD (and the medical devices MDR, IVDR) ?	Since these legislations are the responsibility of other Commission services, we are not in a position to provide an answer. We suggest that you get in touch with our colleagues in DG GROW and DG SANTE respectively

19	Also, any plans to transpose ITU-T X.1811 on Quantum-safe 5G ("IMT-2020" in ITU lingo) for OT in Europe?	Not at present.