ATM CYBER-SECURITY - THE INDUSTRY PERSPECTIVE (WEBINAR)

Question	Answer
Hello. At the end can we get all the support materials on e-mail?	Ruben Flohr The webinar recording and the presentations will be made available on the SESARJU website
Are we going to use MITRE ATT&CK framework?	Tatjana Bolic It is a good resource, but it is not mandated.
What about traditional approach, Identify, Protect, Detect, Respond and Recover?	Ruben Flohr Within the SESAR R&D programme a security risk assessment methdology (SecRAM) is used that indeed looks at all these aspects. Irrespective of the methodology used (ISO, NIST, EUROCAE, etc), these aspects always appear when investigating cyber resilience.
1. Before you consider this as the research topic in the medium- to long term, the developments until now need to be analyzed. Is the system and to what level cyber-secured at the moment. 2. Who are the potential attackers and what their motivation could be?	Tatjana Bolic There is evidence that there is need for improvement. However, this should not become a new topic within ATM - rather we should start merging already established knowledge and practices from the cybersecurity experts in other areas with the needs and specificities of ATM. The MITRE Att&CK compiles the lists of attackers (https://attack.mitre.org/groups/), tactics, techniques and mitiation actions. Here are the EASA news on cybersecurity issues https://www.easa.europa.eu/eccsa/sectorial-news. Another good source of sharing of cyber-threats in aviation is https://www.a-isac.com/
What about adaptive cybersecurity ?	Olivier Segien Thales is working on this area using machine learning and artificial intelligence. This is actually already used within our cyber solutions for data centres and banking domain. This will take time (several years) to be applicable to CNS/ATM systems in operation but seems very promising.
Are ATM, airlines, and airport cyber security interrelated and how?	Olivier Segien The CDM is at least one interroperability mean which can be attacked through several access points.
Why ATM is not already identifed as Essential service? isn't it more important to solve cybersecurity issue of ADSB-B first?	Tatjana Bolic They are already identified. The European Commission characterised CNS/ATM services as Critical services.
Question for presenter: You mentioned AI as a possible solution for shared situational awareness about security. However, a recent ENISA report on self driving car identified AI as one of the critical aspect because of the possible attacks to the reasoning mechanism and its lack of trasparency.	Costas Christoforou The use of AI is already in use in some Data processing systems and will be needed in both the ATCOs WP to help the increased automation and to the ATSEP WP to help decision making on the System Monitoring and control.
Exact measures of added value of improving the current cyber security need to be introduced. How the system is currently vulnerable?	Tatjana Bolic There is evidence that the cyber attacks are constantly taking place. The legacy systems are not cyber-secure. The newer systems take the security into account. The legacy and new systems are operating together, and will continue to do so in the foreseeable future. The cyber-attacks are becoming more and more frequent and more

	sophisticated. Meaning that it will take constant vigilance and evolution to stay ahead of the attackers.
Which is the Industry's approach on developing Cyber Security solutions regarding that the ATM is not just an IT system but a complex sociotechnical Cyber Physical System that includes legacy systems and equipment?	Tatjana Bolic Has answered live.
For Olivier / Thales : Do you propose also Crisis Management Services once the attack has started ?	Olivier Segien Yes, Thales is proposing CSOC to support the end user during an attack.
For Oliver: Doesn't the ATM contain an inherent vulnerability. What are the threshold values when you start acting? Contingency measures are not clear - how are they designed?	Olivier Segien Yes, as most of ATM systems are built with Hardware COTS (eg servers, routers…) and several SW COTS (eg RedHat ..) they contain vulnerabilities. We start acting as soon a vulnerability can lead a cyber threat within the ATM context.For instance the same vulnerability can have an serious impact in one operationnal configuration but not in another configuration. Contingencies are multiples and are built based on the lost operationnal services and contingency plan is often to be amended. it can be done with hardware or software.
Its nice Thales is providing vulnerability management, but the question is how? How do you monitor third party solutions vulnerabilities and how do you assess their applicability in operational context?	Olivier Segien Yes, we can monitor third party solution as soon we have the exact and detailed configuration. We will assess the vulnerabilities within the context of your operational CNS/ATM context.
For Oliver: You mentioned security-by-design in your slides. What level of assurance do you recommend for associated versification and certification?	Olivier Segien Level C to D from NIST levels for critical functions
For Oliver: Is ATM operator and other operators aware about the potential cyber attack and how the proposed solution makes them aware of?	Olivier Segien We have typical training for this population. The training is customised for the ANSP depending on the level they have.
Can an ANSP be held liable for having been compromised by a cyber-attack? (In criminal justice terms, can the victimised be declared liable?)	Costas Christoforou Has answered live.
@ Olivier Our servers come from external suppliers like all our electronic components, is there an extended control of components such as memory or storage devices against installed malware? how is the control done if it exists at the suppliers?	Olivier Segien Yes it can be done for some of them. If the HW or COTS are not too specific or end of life, we are able to follow vulnerabilites . Difficult to answer better without more details, but it should be possible. Write us! Thanks for your question.
Please re-share the thales marketing email, didnt quite catch it.	Olivier Segien marketingatm@thalesgroup.com
For Oliver: Undertaking all this at the new research level needs careful and strong justification by assessing the existing cyber security of the entire system. Do we need and how to worry about at the moment?	Olivier Segien Difficult to answer. This mainly depends on your global system architecture and what kind of interfaces are connected on top of the usual CNS/ATM ones. We will be pleased to discuss further with your at marketingatm@thalesgroup.com
The Thales tooling focusses on detecting intrusions. What about vulnerability detection	Costas Christoforou Has answered live.

to be able to patch before a security event occurs?	
1. Do you consider that the research has to focus on permanent improvement of AeroMacs as it seems that will be standardized soon?	Costas Christoforou and Ruben Flohr Have answered live.
(IFATSEA). 5. Will the tools under development be able to identify potential cyber threats to ATM information systems, and provide to ATM authorities the appropriate information in order to act proactively and through their ATSEP experts to address vulnerabilities ahead of time?	Olivier Segien Yes the tool will be able to identify potential cyber threats to ATM information systems, and provide the appropriate information in order to act proactively . Regarding vulnerabilities, write us @ marketingatm@thalesgroup.com for more information
For Indra: What protection measures are being implemented in iTEC?	Diego iTEC has a dedicated working group integrated by ANSP experts and Indra experts to deal with all the cybersecurity issues within the iTEC versions. The scope of this WG covers both, enhancements of products/technical solutions collected in the CyberSecurity Technical Requirements; and processes collected in our CSMP (CyberSecurity Management Plan). This has been embedded within the iTEC Lifecycle in order to comply with our Security-by-design goal. Moreover this has been complemented with the ISO27001 for Indra ATM iTEC Business Unit. In case of Enaire (the ANSP that you represents), complementing this work, there are also ad-hoc conversations with your CyberSecurity manager for all the new contracts for detailing the ad-hoc topics you need and also for dealing with the ENS (a kind of customized 27001 for Spanish aministrations).
There is a (huge) effort by the EU (EATM) to integrate ATM and UTM. Does the adopted cybersecurity approachs have this into account? Whats is being developed/implemented regarding this aspect?	Olivier Segien Cyber in UTM is becoming a key topic due to the potential very high number of users, connected systems and that most of UTM solutions are cloud/web based. For the time being there is few mandatory requirements or done on a case by case (NIST-800-53 in USA). Thales, and we hope our competitors, implement robust cyber-security measures to protect our solutions and insure that the services and data provided can be trusted by the users and 3rd party systems anywhere at any time. The cyber-security of UTM impacting ATM will come with the future work on ATM/UTM interoperability that has started with SESAR PJ34, unfortunately in this initial step, cyber-security is not part of the project scope. It can be noted that within the USAF project in USA, we are actively studying this issue and working on the design of the overall system-of-systems to address this emerging risk.
For Diego / Indra : In what way do you adress differently the Cyber issues in ATM industry with respect to order industries working with IT ?	Diego We are not reinventing the wheel in ATM but adapting the already existing technologies/processess to the ATM arena. ATM are quite complex systems with non-standard protocols/behaviours part of a complex architecture and with complex product/project lifecycles (i.e. they are not a simple webpage) hence, it requires a complex analysis for using it within ATM. The point that ATM are evolving

	towards mainstream technos/COTS has pros/cons and as one of the 'pros' it open the oppotunity to mainstream Cyber products/solutions.
Quantum technology could reduce risks. Nowhere mentioned. What do the presenters think of that?	Tatjana Bolic The quantum technology has been mentioned in the previous workshops. The summary is that in the post-quantum computing era, the current cryptography can become vulnerable if the systems are not designed to be quantum-safe. Some reading: https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography , https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions , https://www.nature.com/articles/nature23461
Quantum Tech will also bring more risk. Is there a concept of PQC Agility?	IFATSEA We share your concern. We believe that although R&D has addressed some failure modes, regulation does not fully adopt and address these failures in the regulation. Just remember that EU 2017/373 does not require a Safety assesment for the ATM systems but only a Safety Support analysis. In our opinion ,this is not enough and the said regulation must be revisited.
A Remote Tower Center controlling several airports is particularly vulnerable to a cyber-attack, outage of a system or third party service provider, unless contingency procedures for a full RTC failure are established. Can we look forward to regulations in this important area?	Olivier Segien We fully share your point of view on this topic.
Hello, as ATM ANSP how can we assess the vulnerabilities of third party solutions like telecom providers ?	Tatjana Bolic By applying cybersecurity assessment. The ATM Cybersecurity maturity Model Level 1 can be the starting step.
Now that we have established that atm is a complex ecosystem what are the immediate measures on physical layers that ansps should take immediately	Olivier Segien Thales recommends to make a cyber security assessment which will highlight to the ANSP which vulnerabilities shall be corrected immedialty. IFATSEA We do not understand the term 'certified ' since we believe that CNS/ATM systems Certification is exactly what is currently missing. In any case operationally and technically CNS/ATM systems before patching is approved, the impact on the operational performance/operation is needed. This element has not , so far been addressed in depth, with the exeption of the generic assesmnt in the Changes procedure in 2017/373.
How to tackle the cybersecurity in certified ATM safety critical systems, which can not be simply patched, or at least not that quickly like in other IT business systems?	Olivier Segien Indeed, this is true! An ATM system can not be patched like any other IT system. The patch process shall follow the same safety process required for any other patches witch are applied in the system.
ATM is "forced" to use COTS SW. Also SWIM means more standardization. SW and Services commonly use shared 3rd party libraries, dependencies: How to ensure supply chain	IFATSEA We understand that COTS is mainly on the side of Operational systems and networking applications. As such, their use brings in their associated vulnerabilities

security? Regular patching could be problematic- introducing vulnerabilities into systems like in SolarWinds, ASUS, NotPetya cases.	but the impact will be on safety critical applications. It is not an easy task to address while taking into account that Software Safety assurance for software is no longer mandated for ATM appliations. We consider this a serious issue and should be taken up as a task for EASA together with the revision of Software Safety assurrance for CNS/ATM Systems
Thinking of the global nature of ATM service provision (adjacent ANSPs, CSPs, ISPs like NewPENS, etc.), I think that to guarantee a Cybersecured European ATM all of these "actores/authorities" must be globally coordinated by an overlay aurhotity, a EU Security Op Center...would anyone agree?	IFATSEA We believe that EASA should be the overarching authority. Inherently they will have to establish the overarching mechanism to ensure coordination with the specialized national and supranational authorities as well as Operational Partners (ANSPs, airlines, staff associations).