International Civil Aviation Organization

WORKING PAPER

A39-WP/370
TE/159
8/9/16
(Information paper)
English only

ASSEMBLY — 39TH SESSION

TECHNICAL COMMISSION

Agenda Item 36: Aviation safety and air navigation implementation support

A CYBERSECURITY ARHCITECTURAL APPROACH FOR LEGACY- AND SWIM-BASED CNS/ATM SYSTEMS

(Presented by the International Federation of Air Traffic Safety Electronics Associations (IFATSEA))

EXECUTIVE SUMMARY

This paper describes a high level architectural approach to addressing the cybersecurity issue for ANSPs for short and mid-term. Also it provides elements of a long term approach so as to transform and standardize the monitoring of critical technical system processes in order to achieve a fully predictive system awareness in terms of its health, status, both at the level of service provided but also in terms of cybersecurity.

The architecture is aimed at bridging the gap of the lack of specific tools and measures, addressing the integration of cybersecurity in a complex system of systems such as SESAR and NextGen etc.

IFATSEA understands the very high importance of laying down solid and future proof foundations for this scalable system, now, so that it can easily expand and grow in the future. It is felt that one cannot address new challenges such as Cybersecurity with old tools on a purely reactive basis.

This Concept of SMC-SEC was submitted to SESAR Joint Undertaking (SJU) for the Systems Monitoring and Control concept, enriched with elements from IFATSEA Cybersecurity Working group. Operational input from ATCOs has also been incorporated.

Strategic Objectives:	This working paper relates to the Safety, Air Navigation Capacity and Efficiency and Security and Facilitation Strategic Objectives.
Financial implications:	
References:	1. https://www.canso.org/canso-cyber-security-and-risk-assessment-guide 2. http://www.eurocontrol.int/sites/default/files/news/files/NEASCOG-CNS-security-statement.pdf 3. https://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final.pdf 4. http://www.gamma-project.eu/wp-content/uploads/2013/11/GAMMA-overview-and-first-results.pdf 5. https://ifatsea.box.com/v/icao-wp-annex1

1. INTRODUCTION

1.1 Today, most EATMN systems are based on closed networks that are connected between 'trusted' parties. Thus the cybersecurity risk at the level of networking (over copper wire), is minimal. However, with the implementation of SESAR and NextGen this will change radically.

1.2 New business models will lead to different system configurations. For example, the Virtual Center and Remote Tower concepts, decouples the ATCO working position from the Processing technical part which could even be in different states. These changes will need to rethink the issues of SMC (Systems Monitoring and Control) as there will be ATSEP on both sides of the border attending to systems that serve the same purpose (e.g. of providing ATS to a specific airspace) and of course any risks that may rise in the area of Cybersecurity. For example, imagine the situation where there is a 'false target' or spoofing issue with the ATCO Supervisor in one country and the ATSEP SMC Supervisor in charge of the sensors and the ACC Data processing in another country. Addressing this cyber incident would be a challenge given that tools for shared awareness of security threat level and total system state and health awareness, have not been researched and developed yet. What we have at the moment, are ANSPs trying with their own means to handle the situation.

2. DISCUSSION

2.1 The issue of Cybersecurity for ATM is complex as it also includes the physical security at local and remote CNS mission critical installations, the networking elements (space and ground), the ATM specific attack vectors e.g. on Surveillance (i.e. spoofing), jamming of space navigation or RPAS, etc. It is also a worldwide issue since it involves interstate flow of sensitive information.

2.2 In general, the Technical Supervision process operated by ATSEP, becomes aware of events through Systems Monitoring in order to proceed to Control actions as needed. This means that in the case of a degraded mode of operation of one or more CNS/ATM and/or SWIM processes, today, it will have to be solved by the antiquated peer to peer or customary/proprietary monitoring & control text terminals. These only address a specific system status and nothing else, thus failing to detect distributed impact of potential attack vectors and with no global system awareness. In other words, the Total System Approach is missing and has to be addressed, researched, validated, standardized and global specifications be produced preferably by ICAO. (Ref. 1'Detection requires a centralised cyber security operations center (SOC) staffed by experts with up-to-date knowledge of the evolving cyber threat. The SOC must be supported by analysis tools fed by intrusion monitoring …').

2.3 IFATSEA proposes a Technical System Monitoring and Control (SMC) model that refers to beyond state of the art concept, an event object mechanism interfacing with individual systems (or Service providers (e.g. SWIM, Datalink)), with predictive capabilities based on specific sensors activity monitoring (s/w and h/w) and displaying their health status in the SMC domain.

2.4 Related task and Job descriptions as well a training syllabi will also have to be developed for personnel such as ATSEP, ATCO and possibly Pilots.

2.5 Principles of Concept design

2.5.1 The following principles have been considered:

— The effect of the cybersecurity event must not reach the Controller or Pilot (if at all possible)

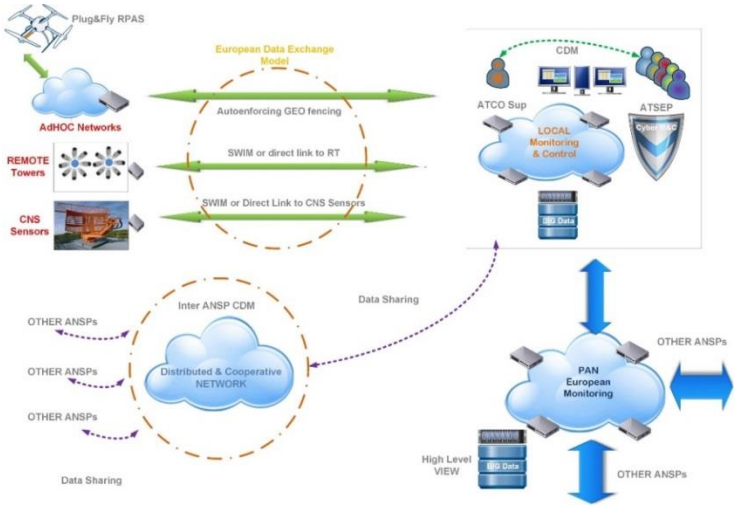
— Cybersecurity events are treated as any other technical event. ATSEP on duty must have the appropriate tools to distinguish whether the event is a Technical failure or Cybersecurity event and make decisions augmented by automated tools.

— Events are not only IT but go far beyond and may include physical elements such as 'signal in space' or RPAS or DoS (Denial of Service). RPAS plug-in to digital network prior to flight thus enabling real time tracking and logging.

— Concepts such as Remote towers integrate C&C in SMC/Cyber. Data is collected, shared and analysed in SMC/Cyber (or SMC_SEC). Cyber-attack vector, pattern recognition and analysis are done locally, Pan-European or globally but at different levels. Big Data systems analyze overall high level Cybersecurity Pattern and Attack Vector Recognition.

— Due to the need for real-time network reconfiguration in an event of intrusion, decision capability is between ANSPs. Pan-European or global function is predictive and informative whereas local functions include decision making and control.

— The rules and criteria at CEP (Complex Event Processing) to provide the desired output will be set up by experts (ATSEPs, ATCOs) of local ANSP level who will take into consideration local circumstances.



2.6 **Technical description**

2.6.1 A cybersecurity related event, is considered as any other event, taking of course into account the type may be of a transversal nature, impacting more than one process or service in the ANS environment.

2.6.2 The system's technical health events, including Cyber events, must be addressed by feeding a Complex Event Processing (CEP) (see Fig.1) engine being implemented at Local ANSP level in the Technical Department (CNS/ATM). According to the Cyber and System's health related predefined criteria(rules), the outcome of this CEP has to be treated accordingly and in any case as close as possible to real time. So Cyber threats or suspicious activities detected will be immediately addressed locally and communicated at a higher level (National) or further through to supranational entities.

2.6.3 The above mentioned configuration for implementation of CEP at local ANSP level is imperative for the following reasons:

— The number of sensors and systems embedded in CNS/ATM, will be producing large numbers of messages (events) needing to be treated by corresponding CEP processes, in order to ensure lower vulnerability of the whole system, high probability of detection and of course minimum false alarms. (note: Full concept at IFATSEA e-library ref. 5)

— By tackling the Cyber events locally at ANSP CEP level, the capability of filtering out the ones necessary to be transferred to a higher level will be ensured, resulting to strengthening the security of a second level.

— The cost benefit of including the CEP dealing with cybersecurity events in the Tech supervision (SMC) context is promising.

— It must be noted that the initial trigger event, first of all has to be identified and categorized whether it is a technical failure, a security incident or a combined case.

2.6.4 What is beyond the current state of the art and is proposed by IFATSEA, is the definition of a System Health SMC Object. This object will integrate further a Security Data Object in order to acquire a continuous holistic picture of the 'real time' system status, leading to an in depth system wide awareness with prediction capabilities.

2.6.5 The filtered output of the events created by these objects will be displayed on SMC Presentation Layer to the screen of the ATSEP (Technical) working position (A-CWP) on duty, supported by decision making tools. This will allow the trained ATSEP on duty to take the necessary actions, including Control facilities of H/W or S/W or information dissemination to other related entities, within or outside the ANSP level (e.g. Security threat level to ATCO supervisor) or to National Security entities. Therefore, the Complex Event Processing & Analysis will have to be incorporated as a 'delta' to ATSEP SMC level. Needless to say that the human operator (e.g. ATSEP, ATCO) dealing with the security events must be trained and specialized in addressing security issues in the CNS/ATM environment.

3. THREAT SCENARIOS

3.1 These can be local or distributed, the most dangerous being a distributed collection of events which may appear innocuous by themselves but as a whole may permit e.g. a Zero-day attack vector. This can only be detected by sharing of data and pattern recognition algorithms at local and global level. These can be related to Airspace, IT, Infrastructure/installations or access control systems as well as Intrusion detection systems or a combination of the above. *(ref. 4)*

4. COST EFFECTIVENESS

4.1 The IFATSEA approach takes into account the particularities of the CNS/ATM environment and the safety and time criticality of ANS services. This is not addressed as a purely IT Security project but with a holistic approach encompassing Airspace related, IT related and Infrastructure/installations or access control systems tailored to the ANS environment. In the forthcoming automation era, SESAR and NextGen being Sociotechnical System of Systems, it will be very difficult to address issues like cascade failures which are a potential reality due to the tight coupling, interoperability and interrelation of the new processes.

5. CONCLUSION

5.1 Designing systems with Cybersecurity in mind, enhanced with SMC_SEC Object within a SMC_XML object over secure protocols, will constitute a paradigm shift and create a strong Cybersecurity Capability for ANSPs.

5.2 ICAO is requested to take note and evaluate the content of this IP as a bottom up proposal driving further studies in the cybersecurity domain.

5.3 This work has been done concentrating on the more developed highly automated Future ATM Systems and as such lacks as yet critical elements on the criteria relating to the realities of regions like Africa and the Pacific, these while being impacted by the output of systems like SESAR and NEXTGEN also have their local and very specific realities, requirements and limitations.

5.4 IFATSEA is working on collecting data and working with professional organizations from these areas to update this present document.

5.5 Furthermore, IFATSEA is available to further explain and contribute to the study of the high level requirements definition of such a System Health SMC Object.

— END —