SAE INTERNATIONAL

SAE EDGE™
RESEARCH REPORT

Unsettled Topics Concerning Airport Cybersecurity Standards and Regulation

Aharon David

SAE EDGE™
RESEARCH REPORT

Unsettled Topics Concerning Airport Cybersecurity Standards and Regulation

Aharon David
AFUZION-InfoSec

SAE INTERNATIONAL®

Warrendale, Pennsylvania, USA

About the Publisher

SAE International® is a global association of more than 128,000 engineers and related technical experts in the aerospace, automotive, and commercial-vehicle industries. Our core competencies are lifelong learning and voluntary consensus standards development. Visit sae.org

SAE EDGE™ Research Report Disclaimer

SAE EDGE™ Research Reports focus on topics that are dynamic, in which knowledge is incomplete, and which have yet to be standardized. They represent the collective wisdom of a group of experts and serve as a practical guide to the reader in understanding unsettled subject matter. They are not meant to provide a recommended practice or protocol. The experts have assembled as a community of practitioners to contribute and collectivize their thoughts and points of view. These are not the positions of the institutions or businesses with which they are affiliated, nor is one contributor's perspective advanced over others. SAE EDGE™ Research Reports are the property of SAE International, and SAE alone is responsible for their content.

About This Publication

SAE EDGE™ Research Reports provide state-of-the-art and state-of-the-industry examinations of the most significant topics in mobility engineering. Contributors to SAE EDGE™ Research Reports are experts from academia, government, industry, and research who have come together to explore and define the most critical advancements, challenges, and future direction in areas such as vehicle automatic unmanned aircraft, cybersecurity, advanced propulsion, advanced manufacturing, Internet of Things, connectivity, and quantum technology.

Related Resources

SAE EDGE™ Research Report: Unsettled Topics Concerning Airworthiness Cybersecurity Regulation by Aharon David
https://saemobilus.sae.org/content/EPR2020013/

SAE Team

Frank Menchaca, Chief Growth Officer
Michael Thompson, Director of Standards, Information, and Research Publications
Monica Nogueira, Director of Content Acquisition and Development
Beth Miller Dibeler, Product Manager
William Kucinski, Managing Technical Editor

EPR2021020
ISSN 2640-3276
e-ISSN 2640-3284
ISBN 978-1-4868-0368-2

To purchase bulk quantities, please contact: SAE Customer Service

E-mail: CustomerService@sae.org
Phone: 877-606-7323 (*inside USA and Canada*)
+1-724-776-4970 (*outside USA*)
Fax: +1-724-776-0790

https://www.sae.org/publications/edge-research-reports

About the Editor

Aharon David is a co-founder and partner of AFUZION-InfoSec, a global services, consulting, and training company specializing in aviation cybersecurity certification. He is also a speaker and trainer on aviation cybersecurity certification for organizations such as SAE International, the American Institute of Aeronautics and Astronautics, IEEE, Aerospace Tech Week, and others. He is a member of all United States and European standard-making committees for aviation safety-critical electronic systems, cybersecurity, artificial intelligence, and unmanned aircraft systems (UAS), including SAE's S-18, G-32, G-34, and others; RTCA's SC-216, 224, and 228; the European Organisation for Civil Aviation Equipment's WG-72, WG-105, and WG-114; and others.

For the last decade, he has been an advisor to Israeli government authorities, such as the Civil Air Authority of Israel (CAAI), on subject matters such as UAS, avionics software, cybersecurity, and more.

He is an aerospace engineer and holds a master's of business administration in information systems/technology management with four decades of hands-on engineering management and executive experience with the Israeli Air Force (IAF), Israeli Ministry of Defense, CAAI, and others. His past roles include commander of the IAF's Avionics and Control Software Centre and head of the Israeli Missile Defense Organization's System Engineering and Interoperability Department (among others).

He combines perspectives from the civilian and defense sectors in technology, business management of large organizations, and passenger aircraft and UAS aviation development and certification.

contents

Atosan/Shutterstock.com

Unsettled Topics Concerning Airport Cybersecurity Standards and Regulation

Abstract

A large international airport is a microcosm of the entire aviation sector, hosting hundreds of different types of aviation and non-aviation stakeholders: aircraft, passengers, airlines, travel agencies, air traffic management and air traffic control, retail shops, runway systems, building management, ground transportation, and much, much more. Their associated information technology and cyber-physical systems—along with an exponentially resultant number of interconnections—present a massive cybersecurity challenge.

Unlike the airport physical security challenge, which was treated in earnest throughout the last decades (to the point where physical intrusions are now extremely rare), cyber-attacks on airports keep coming "fast and furious." This might come as a surprise, as most airports, nowadays, employ very capable chief information security officers (CISOs) and state-of-the-art tools. However, deeper analyses reveal that most airport CISOs lack some of the most essential means to confront such cyber-attacks.

These missing means are not technical tools, but rather holistic regulatory directives, technical and process standards, guides, and best practices for airports' cybersecurity—even airport cybersecurity concepts and basic definitions are missing in certain cases.

Similar to the previous SAE EDGE™ Research Report on "Unsettled Topics Concerning Airworthiness Cybersecurity Regulation," [1] this present report offers a deeper analysis of these issues and their causes, focusing on four main unsettled domains: the unique characteristics of airports in general, the specific cybersecurity challenges posed by airport, and the missing definitions and conceptual infrastructure for the standardization and regulation of airports cybersecurity. This last item includes the gaps and challenges in the existing guides, best practices, standards, and regulations pertaining to airport cybersecurity.

Finally, practical solution-seeking processes are proposed, and some specific potential frameworks and solutions are pointed out whenever applicable. It is the intention of this report, with its insights and observations, to assist regulators, applicants, and standard-makers throughout the 2020s with the development of airport cybersecurity guides, best practices, standards, and regulation—which, in turn, will enhance airport cybersecurity.

NOTE: SAE EDGE™ Research Reports are intended to identify and illuminate key issues in emerging, but still unsettled, technologies of interest to the mobility industry. The goal of SAE EDGE™ Research Reports is to stimulate discussion and work in the hope of promoting and speeding resolution of identified issues. SAE EDGE™ Research Reports are not intended to resolve the challenges they identify or close any topic to further scrutiny.

AHARON DAVID
Chief WHO (White Hat Officer)
AFUZION-InfoSec

ISSN 2640-3536