

Cyber State Requirements for Design and Validation of Trust in the Critical Transportation Infrastructure

Tim Ellis, Michael Locasto, David Balenson

▶ **To cite this version:**

Tim Ellis, Michael Locasto, David Balenson. Cyber State Requirements for Design and Validation of Trust in the Critical Transportation Infrastructure. 14th International Conference on Critical Infrastructure Protection (ICCIP), Mar 2020, Arlington, VA, United States. pp.69-83, 10.1007/978-3-030-62840-6_4 . hal-03794631

HAL Id: hal-03794631

https://inria.hal.science/hal-03794631

Submitted on 3 Oct 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License



This document is the original author manuscript of a paper submitted to an IFIP conference proceedings or other IFIP publication by Springer Nature. As such, there may be some differences in the official published version of the paper. Such differences, if any, are usually due to reformatting during preparation for publication or minor corrections made by the author(s) during final proofreading of the publication manuscript.

Chapter 1

TOWARDS CYBERSTATE REQUIREMENTS FOR DESIGN AND VALIDATION OF TRUST IN CRITICAL TRANSPORTATION INFRASTRUCTURE

Tim Ellis, Michael Locasto and David Balenson

Abstract The National Transportation Safety Board (NTSB) is charged with investigating transportation related accidents in aviation as well as railroad, highway, marine, and pipelines. The increased integration of Operational Technology (OT) systems with traditional Information Technology (IT) systems brings both increased vulnerabilities and risk of cyber-related issues. In this paper we explore requirements for trust in critical transportation infrastructure (CTI) in light of increased OT and IT integration. NTSB investigations require trustworthy data to make effective decisions about accident causes and remedies. We focus on the specific use case of internal aircraft systems and their data in accident investigations. While current commercial avionics systems employ very reliable serial bus architectures, these systems and their components were not designed with cybersecurity issues in mind. Cyberstate mechanisms such as software attestation and data protection must be designed into CTI and validated to support trust requirements for accident investigations. In addition, we recommend ensuring secure collection of additional data to aid in investigations, employing anomaly detection techniques to detect potential cyber-related attacks or make data collection more efficient, and establishment of a vulnerability registry and risk assessment system, similar to those in the IT domain, to better share and expose potential cyber-related issues.

Keywords: Transportation infrastructure, NTSB investigations, trustworthy data

1. Introduction

The National Transportation Safety Board (NTSB) [24, 27] investigates accidents and incidents in critical transportation infrastructure

(CTI), such as aviation as well as railroad, highway, marine, and pipelines, and plays a crucial role in maintaining and improving the safety and security of such systems over time. Thorough investigations restore and bolster public confidence in the reliability and safety of this infrastructure. The conclusions and recommendations of these investigations are seen as impartial and carry weight precisely because these investigations are undertaken in a deliberate, forensic manner that is not influenced by external considerations or by poisoned data. Investigations proceed on an assumption that operational data both carried and captured by computer and communications equipment forming a part of the system under investigation are trustworthy. We see, however, some potential gaps in the validity of this assumption, particularly as critical transportation infrastructure incorporates IT components as part of their Operational Technology (OT) systems.

OT control systems for industrial operations, energy distribution and control, and aircraft operations are rapidly evolving in sophistication and automation. These systems, many originally built on technologies that originated decades ago, are becoming increasingly vulnerable to accidental or intentional attacks via electronic (cyber) means. Minimizing these problems, as well as being capable of differentiating between identification of normal component wear or failure and malicious cyber activities, is becoming increasingly important to OT operators and incident investigators to develop safe and effective responses and countermeasures.

The purpose of this paper is to assess the requirements space for acquiring trustworthy data so that investigations into the causes of accidents or incidents in CTI can be reliably conducted and the findings and any safety recommendations are accurate and trustworthy. For the sake of concreteness, we limit the focus here to the internal avionics data systems of commercial aircraft. We examine the extent of their operational and investigative support capabilities and review cyber-related considerations that could be included in aviation system design and implementations. We also provide some guidelines and recommendations to be considered by the commercial aviation industry, standards authorities, and incident investigation agencies to improve the cyber resilient posture of onboard avionics systems and the trustworthiness of data collected by these systems and used in accident investigations. Our sample review of recent aviation accident and incident reports by the NTSB [25] reveals that, while none of the commercial aviation accidents over the last 10 years were likely due to cyber-related causes, there is a high dependence on data collected by subsystems potentially vulnerable to cyber interference. In addition, there appears to be a high degree of implicit trust in the validity and integrity of these data sources used

for investigation, and the only recognized vulnerability to data integrity seems to be fire or physical damage due to the accident. Thus, these data are primarily protected with byzantine robustness measures that protect against dependency failures, but not necessarily against active adversaries. As a result, there is a need for better attestation of the data and software used in operations as well as mechanisms to preserve such information for forensic investigations. Finally, there are promising data collection and analysis opportunities, including the possible use of advanced machine learning techniques to monitor aviation or OT bus traffic that could detect patterns of interest for alerting, analysis, or even real-time detection or protection of the system from cyberattacks.

Section 2 describes the challenges presented by today's avionics data and communications systems in implementing modern cyber resilience and trust. Section 3 introduces the concept of trust, in relation to the data collected by these systems and its use in forensic investigations. Section 4 discusses some mechanisms that could be used to preserve and protect these data by applying known techniques from today's cybersecurity community. Section 5 summarizes our observations of these data protection techniques and their potential for application to the commercial aviation industry and, in particular, forensic investigation uses. Section 6 provides our overall observations and potential next step recommendations. Section 7 covers related work. Finally, we conclude the paper in Section 8 and suggest areas for future research.

2. Aviation Data Challenge

Aircraft systems, like most OT systems, employ a complex mix of components to sense, control, automate, communicate, and monitor their operations. These components contain both hardware and software-based programmable logic, memory, and communications functions. Investigating the potential cause(s) of a system malfunction or anomalous incident necessitates inspection and assessment of the operational state and associated data of each relevant component over the timeframe before, during, and after the incident, to the extent possible. Standard IT-based networking and data extraction tools may be applicable here, but will need to be either adapted, or redesigned to provide the kinds of data needed by accident investigators.

The procedures for investigating these components individually are well established and often augmented by vendor provided tools, procedures and guidance, or even by the vendors directly collaborating with the NTSB in an investigation (see, for example, the Air France 447 report describing manufacturer support in extracting data from mangled

storage devices [8]). But when considering the system of components as a whole; and when considering the potential for intentional cyber related causes; it is also necessary to monitor, track, and assess the inter-component communications to understand the "conversations" taking place on the interconnecting message networks and buses. Understanding these protocols and what constitutes "normal" and "abnormal" patterns could be used to help identify and assess the potential for malicious traffic introduced onto the communications fabric—either by direct injection onto the bus, or via compromised system components. Analyses of these message traffic patterns could be performed real-time, onboard with components operating in an incident detection and possible preventative mode, provided sufficient onboard processing and analytic models exist. Or, this analysis could be conducted forensically and offboard in an incident investigation or response mode to recreate the actual sequence of messages and events from stored traffic data.

These OT systems typically communicate using serial standards interface buses. These types of networks can be complex and require specialized equipment to effectively monitor and extract traffic data. In the ARINC 429 standard [38, 1], the standard used on higher-end commercial and transport aircraft today, each bus consists of one transmitter component node, or Line Replaceable Unit (LRU) and up to 20 receiver LRUs. Bi-directional communications between LRUs requires a transmit bus and receive bus for each LRU. Buses may be interconnected by LRUs specifically designed to pass messages from their input port to their output ports. Thus, a typical aircraft has many interconnected buses connecting dozens of LRUs. These include controllers; managers; monitors; or recorders of a number of subsystems on an aircraft; such as flight management and controls, communications, engine and fuel controls, landing systems, or environmental controls. Collecting a coherent session of communications will often require collecting the traffic on multiple bus segments simultaneously, with synchronized and secure time stamps to allow temporally accurate understanding and review to accurately reconstruct all the elements of an accident or incident.

As the ARINC 429 standard protocols have evolved over time, additional functions have been added to improve performance and capabilities by overloading existing functions to maintain backward compatibility. Consequently, interpretation of the message data words is highly contextual to the data and LRU's involved. This level of context dependency can open vulnerabilities to problematic or "weird machine" behaviors. It is recommended that a language-theoretic security (LangSec) analysis [19] be conducted to determine possible vulnerabilities intro-

duced by context dependencies and streaming message handling as well as mitigation strategies for the ARINC 429 protocol.

3. Data Trustworthiness

To conduct reliable and accurate investigations, the system under consideration must have verifiable levels of trust in the software it is running, and in the capture and protection of any data produced. For software-based logic components to operate reliably, it is necessary to ensure that only certified, trusted software is loaded, maintained, and executed on each component. This is an area that has been extensively addressed in the IT world through secure methods to ensure the integrity of software before installation and prior to each use. These attestation techniques include the use of cryptographic hashing and time stamps on 'gold' releases of firmware and supporting data, software attestation checks on these hashes each time a system is started, or use of Trusted Platform Module (TPM) [36] hardware in the construction of LRUs for automated attestation in the device. Additionally, the use of Hashed Message Authentication Codes (HMAC) [18] for internodal communications can provide additional assurance that a code segment or update is from a reliable source and has not been tampered with either through fabrication at its source or modification in transit—particularly when combined with code signing techniques. It may be worthwhile examining how such code and updates can take advantage of The Update Framework (TUF) for securing software update systems [20] and its UPTANE variant for securing software updates for automobiles [21].

A collaborative process is needed to ensure that the investigative organization has access to trusted data for investigations. Table 1 illustrates a common, cyberstate checklist approach for defining the requirements in a system to support trusted operations as well as trusted state data for post operations analyses. Here we only sketch a few items to give an indication of the overall structure of the checklist. A real checklist would greatly expand on the options here and define flow between the assurance statements. A tool such as this should be used to define, review and verify that NTSB investigation trustworthiness needs will be met by avionics systems design and implementations. A set of truth statements provides a list of assertions that the NTSB requires to be satisfied as true or at a high level of probability, as indicated in the Assurance column, e.g., True or False, or Prob(X). The appropriate protection mechanisms to ensure these statements will be met, along with specific procedures or equipment needed for implementation, is provided by the equipment manufacturers and operations organizations. Together, these organiza-

tions must also prioritize the requirements to achieve the most impact within available resources and schedules.

Table 1. Example cyberstate requirements checklist.

Statement	**Assurance (Binary or Continuous)**	**Protection Mechanism**	**Specific Procedures (or Equipment)**	**Initial Priority**
Recorded data is unmodified	True	Timestamp and hash	Digitally sign and hash all data in the FDR	1
All bits of flight critical firmware were gold	True	Software attestation, TPM, paper log?	Firmware boot/load attestation check, TPM in hardware	2
No LRU code corruption	True	Hash of the gold software copy	Compare code hash with gold hash	2
No messages of abnormal origin	Prob(X>.99)	HMAC per message	Attestation of origin's ability to "speak" those messages	3
No injected messages	True	HMAC per message	Verification of message HMAC against trusted codes	4

4. Data Protection and Evidence Preservation

Building trust in the operational data used for forensic investigations requires considering protection of the data throughout its lifespan. Table 2 provides a notional assessment of the current state of data protection, in terms of confidentiality, integrity, and availability of digital data in storage, processing, and communications subsystems. For this assessment, confidentiality is the ability to allow only authorized entities and devices access to the data and services involved, integrity is the ability to ensure that the data has not been tampered with and can be trusted to be accurate, and availability is the ability to maintain and access

the data when needed. The data domains are further divided into major subtypes: Persistent and volatile storage, static code and dynamic behaviors for processing, and both individual message level and multi-message communication patterns. Generally speaking, these subtypes map to static and dynamic system properties, respectively. The entries for each row or column in the table provides typical mechanisms that could be used to provide the associated data protection. Each entry is given a notional assessment indicating, in general, whether these mechanisms are being typically used in current aircraft data systems: not typically used (*italic text*), some or limited use (regular text), or in common use (**bold text**). This assessment is based on a variety of publicly available vendor and industry standards information and background knowledge of the authors and is not meant as a rigorous or comprehensive evaluation. As implied by the table, however, there are a number of areas where improved data protections might be used to better safeguard critical data. In avionics OT, as in much of IT today, there are limited protections in place for the dynamic aspects of storage, processing, and multi-message communications monitoring and threat detection. Further, a more rigorous assessment of these risk states is recommended and should be conducted, along with the recommended data protection improvements. This would lead to an enhanced cyber standard reference for the NTSB's investigation processes as well as a guide for improving future avionics component data protection levels.

5. Data Collection and Analytics

Capturing the network or message bus traffic could be an effective means for both monitoring the health of the system through message pattern detection and providing a store of secure and accurately time stamped messages for analysis of potential anomalies after a flight or incident. To support these data collection needs, it would be necessary to capture and store all or most parts of the bus message traffic. Given the typical volume of data flowing on OT system networks such as aircraft buses, it may be necessary to be selective of what to store based on careful pattern analysis. Naturally, down-selection or sampling of messages poses the risk of missing information related to a computer attack or malfunction. This is an area that could evolve over time as more knowledge is gained about normal and abnormal message traffic and related technologies advance.

Functional data collection requirements include an ability to connect to many separate data buses at multiple points and collect the traffic flowing on each, along with associated time synchronization data, to

Table 2. S-P-C x C-I-A matrix.

Subsystem		**Confidentiality**	**Integrity**	**Availability**
Storage	**Persistent**	*Encryption*	**Hash, Timestamp**	Redundancy
	Volatile	*Access Controls*	**Hash, Timestamp**	**Backup**
Processing	**Static Code**	*Encryption*	Trusted Boot, **Hash/ Timestamp,** *Trusted Boot (TPM)*	**Backup**
	Behavior	Access Controls	Dynamic Behavior Measurement	Heartbeat
Communication	**Message**	*Firewalls, Access Controls*	Hash/ Timestamp, *Hashed Content, Hashed Timestamp, Trustworthy Time Source*	*Firewalls,* Redundancy
	Pattern	*Chaff, Privacy*	*Trustworthy Time Source*	*Pattern Detection*

be able to analyze temporally dependent messages and events. This collected data must include hashing to protect the data from subsequent modifications or tampering. Such a secure data collection regime must also deal with the challenges of authenticity and key distribution to properly handle the long lifetimes of secrets while ensuring the safety of operations throughout the life of the system. Additionally, it could be advantageous if this collected data, or some relevant subset or metadata, is transmitted over the air or other network as available to a ground-based collection repository to allow more extensive investigation and analysis in the event the aircraft or system is damaged or otherwise unavailable for retrieval of collected data onboard.

Data analysis requirements include the ability to integrate all time-synchronized data, collected from multiple buses for event 'replay' and simulation analyses. Further, if sufficient processing capabilities are available onboard the aircraft or operational system, traffic pattern analysis would also allow for the detection of possibly anomalous activities—

or at least more efficient storage of data by saving only the data around any anomalous traffic patterns for particular operational regimes (e.g. taxi, takeoff, departure, climb, cruise, descent, approach, landing) for later analyses.

In addition to the current sets of command, control, and monitoring time-stamped data that are being collected by the Flight Data Recorder (FDR) [26, 28] for flight, propulsion, power, communications, and environmental systems, cyber-relevant data should also be collected for later use and analysis. This data could include the following:

- Select addressed (labeled) messages for key devices. This allows for capturing more of the "conversations" between specific LRU devices, and not just specific commanded or sensed states of aircraft components
- Software attestation log data (at load/startup, and at periodic intervals) to record and ensure that the 'proper' software or firmware is being executed
- "Heartbeat" hashed messages from select LRU devices to monitor or recreate component health. These messages could also include lower level health status or content pattern data such as processor, communications hardware, memory, or other storage sub-components of specific LRU devices to ensure consistency with baseline models and to aid in forensic analyses.
- LRU-generated anomaly data. For example, malformed messages the LRU received and would have otherwise discarded as non-compliant. This type of data could be part of a new signature of a malicious attack and would be useful in post event analysis as well as future investigations and model development.

Additionally, to more effectively track issues and vulnerabilities related to OT systems, a vulnerability tracking registry, similar to the MITRE Common Vulnerabilities and Exposures (CVE) catalog for IT systems and software [35], would allow the community to share and address discovered cyber related issues in a more effective and timely manner by leveraging the collective knowledge across the industry. Similarly, a risk evaluation system, such as the Risk Scoring System [30] developed by QED Secure Solutions, would provide a reliable and vetted means to establish the criticality and potential severity of a given risk or vulnerability as it relates specifically to the safety of operations of the aircraft or other OT system.

6. Recommendations

The NTSB could improve the robustness of aviation data systems to ensure the intended avionics functions are being executed properly onboard commercial aircraft. It should also ensure that in the event of an accident or incident, the investigation into the causes can be reliably conducted using collected data—and the findings and any resulting safety recommendations are accurate and trustworthy. The following set of recommendations could improve both the safety and security of operational avionics systems onboard commercial aircraft, and also improve access and trustworthiness of data needed for reliable post-accident investigations.

- Improve data collection and protection to increase trust in post-event investigations. Storing more of the data flowing on aircraft data buses by extension of the current Flight Data Recorder approach would support more detailed cyber-related analyses of the events leading up to, during and immediately following an accident. Storing all data on a typical commercial aircraft may be infeasible. However, starting with the most critical subsystems and potentially using anomaly detection techniques, described below, to focus the data collection could provide a reasonable and phased approach.

- Apply attestation techniques for the firmware running on avionics devices. Digitally sign all device firmware to provide reliable means for aircraft maintenance personnel to ensure only the certified software and hardware are being operated. This level of attestation will need to be designed into the device hardware and software architectures to ensure that each time the device is powered up, it runs a trusted attestation process to ensure the correct firmware is being loaded and executed.

- Establish a cyberstate issue tracker to collect and share findings about potential issues or vulnerabilities in devices or firmware. Borrow an effective practice from the IT world by capturing salient information about discovered potential vulnerabilities and associated information such as component model and version numbers, configuration settings, and relevant details related to integration with other devices. This system should include a mechanism to score each issue as to its potential impact on flight operations and safety, and not simply its potential for component operations disruption, to aid in prioritization of remedial actions by manufacturers, operators, and maintainers.

- Develop advanced data analytics to better detect anomalies and potential attacks. Consider both on-board and post-flight analytics approaches. Investigate use of currently available machine learning techniques to learn the typical patterns of message traffic over various flight and operational regimes, and use these trained models to conduct anomaly detection, either in real-time if sufficient processing capability exists on-board, or in post-flight evaluations to both find potential anomalies for follow-up actions, as well as for continual training and improving the anomaly detection model.
- Review the ARINC protocols for potential security risks considering both advanced functions being added to the latest avionics devices, as well as the increased use of more traditional IT technologies in these historically OT systems. Conduct a language-theoretic security (LangSec) analysis [19] of protocols and messages to identify potential protocol vulnerabilities and ensure context-free and valid message processing.
- Add cyberstate requirements to equipment designs to support NTSB investigation processes. The avionics vendors and NTSB should work together to define a core set of cyberstate assertions that are needed for reliable investigations and trustable findings, and make sure these requirements are implemented in the next generation of equipment.

7. Related Work

The focus of this paper is on cyber-related aspects of NTSB investigations in transportation accidents and incidents and requirements to ensure trustworthy cyber-related data are available to support their investigations. While it is possible some suggested actions and approaches are already under consideration by the avionics industry, we are not aware of any such efforts.

A November 2017 Atlantic Council report on Aviation Cybersecurity [9] explores the increased digitization in the aviation industry, including aircraft as well as air traffic management, airports, and their supply chains. The report seeks to increase awareness in and the public discussion around the need for increased cybersecurity. Among the report's recommendations are "Improve Agility of Security Updates," "Design Systems and Processes to Capture Cybersecurity-Relevant Data," and "Incorporate Cyber Perspectives into Accident and Incident Investigations." The report stops short of enumerating detailed requirements. This paper suggests a method of providing overall structure to this

problem space by introducing the matrix of confidentiality, integrity, and availability with storage, processing, and communication. This structure enables us to do two things. First, it provides a way for the aviation and cybersecurity communities to understand the defined boundaries of the problem. These communities need to limit the problem scope so they can then prioritize which gaps to most urgently address by incorporating information security technology (e.g., cryptographic-strength integrity mechanisms) into the airframe and integrating the resulting data into investigation procedures. Second, we identify the new requirement to securely store ongoing measurements of both network provenance (message origin authentication and message path validation; similar to routing security) and dynamic device behavior (i.e., the runtime behavior of embedded device code, not just its firmware hash). In doing so, we assist the ongoing discussion reflected in [9] about the requirements needed to ensure trust in cyber-relevant aspects of investigations.

Recent work by Roberto Sabatini, Royal Melbourne Institute of Technology University, reviewed the increased use and reliance on Information and Communication Technologies (ICT), the challenges associated with airborne data networks, and the need for increased cybersecurity focus in civil aviation [33].

There is a significant body of work around the concepts of cyber resilience, resilient systems, and resilient trust (see, for example, [23, 7, 6, 5]) that can be leveraged to help protect critical data in aircraft storage, processing and communications subsystems. Similarly, there's also a large body of work around the digital forensics [39, 15, 12**?**], including preservation of evidence and chain of custody, that can be applied to cyber-related data needed for accident and incident investigations.

Many organizations provide cybersecurity and incident response services, including the new Cybersecurity and Infrastructure Security Agency (CISA) with the U.S. Department of Homeland Security (DHS) [10], which houses the National Cybersecurity and Communications Integration Center [11] and subsumes the former US-CERT [37] and ICS-CERT [17]. Many commercial organizations offer consulting and incident response services and teams as well. There's a growing body of academic research and work on incident response technologies and tools and on effective incident response teams [14, 13, 22, 29, 3].

In recent years, a number of people have proposed and argued for an NTSB-like organization to investigate cybersecurity incidents [16, 31, 4, 32, 34]. While such an organization may be necessary to spearhead investigations into accidents and incidents involving critical infrastructure across the board, such a new organization, as well as, the

NTSB would need appropriate means to ensure availability of trustworthy cyber-related data to support their investigations.

8. Conclusions

Critical Transportation Infrastructure must be capable of ensuring proper functional execution and reliably capturing and protecting operational data in order to support trustworthy forensic analysis in the event of a failure or accident. However, operational technologies employ specialized architectures and may not support the direct use of established data protection mechanisms routinely employed in more traditional IT systems. Therefore, it is necessary for OT communities to review their data protection posture and identify areas for improvement where either traditional IT protection mechanisms can be adapted, or where completely new tools and techniques are needed due to the unique properties and constraints of the OT systems.

This paper reviewed the state of data protection for internal aviation data systems (avionics) as an example critical transportation infrastructure system. Recommendations were made for several areas of improvement to ensure intended functions are being executed properly, and to provide the NTSB, the organization responsible for investigation of aviation related incidents or accidents, with trustworthy data to produce trustworthy findings. These areas include improved and increased data collection and protection to improve trust in post event investigations, use of attestation techniques for the firmware running on avionics devices, a cyber issue tracker to collect and share findings about potential issues or vulnerabilities in devices or firmware, development of data analytics to better detect anomalies and potential attacks, LangSec analysis of protocols and messages to ensure context-free and valid message processing, and the addition of cyberstate design requirements to support NTSB investigation needs.

Future avenues of research could include development of enhanced flight data recorder requirements and prototypes, feasibility of adding attestation techniques to avionics devices, machine learning model development for message patterns and anomaly detection, LangSec analysis of the ARINC 429 protocol, and research and development of a set of NTSB cyberstate requirements in coordination with avionics manufacturers.

Acknowledgements

This work was sponsored by the U.S. Department of Homeland Security (DHS) Science and Technology (S&T) Directorate under Con-

tract No. HSHQDC-16-C-00034. The authors thank DHS S&T Program Manager, Mr. Gregory Wigton, for his guidance and support. The National Transportation Safety Board (NTSB) did not sponsor the work nor did they participate in the work. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of DHS or NTSB and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DHS, NTSB or the U.S. government.

References

[1] Actel, ARINC 429 Bus Interface, Mountain View, California, USA (`www.actel.com/ipdocs/CoreARINC429_DS.pdf`), 2006.

[2] D. Aitel, Daily Dave Mailing List (`seclists.org/dailydave/`).

[3] J. Arthorne, Expect the Unexpected: Preparing SRE Teams for Responding to Novel Failures, presented at *SREcon19 Europe, Middle East, Africa* (`www.usenix.org/conference/srecon19emea/presentation/arthorne`), 2019.

[4] S. Bellovin, The major cyberincident investigations board, *IEEE Security and Privacy*, vol. 10(6), pp. 96–96, 2012.

[5] D. Bodeau and R. Graubart, Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls, MTR130531, The MITRE Corporation, Bedford, MA (`www.mitre.org/sites/default/files/publications/13-4047.pdf`), 2013.

[6] D. Bodeau, R. Graubart, W. Heinbockel and E. Laderman, Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques, MTR140499R1, The MITRE Corporation, Bedford, MA (`https://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf`), 2015.

[7] D. Bodeau and R. Graubart, Cyber Resiliency Design Principles: Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines, MTR170001, The MITRE Corporation, Bedford, MA (`www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf`), 2017.

[8] Bureau d'Enquêtes et d'Analyses (BEA) pour la sécurité de l'aviation civile, Final report on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by

Air France flight AF 447 Rio de Janeiro - Paris, Le Bourget Cedex, France (www.bea.aero/docspa/2009/f-cp090601.en/pdf/f-cp090601.en.pdf), July 27, 2012.

[9] P. Cooper, Aviation Cybersecurity: Finding Lift, Minimizing Drag, Atlantic Council, Washington, DC (www.atlanticcouncil.org/in-depth-research-reports/report/aviation-cybersecurity-finding-lift-minimizing-drag/), 2017.

[10] Cybersecurity and Infrastructure Security Agency (CISA), Arlington, VA (www.cisa.gov/).

[11] Cybersecurity and Infrastructure Security Agency, National Cybersecurity and Communications Integration Center (NCCIC), Arlington, VA (www.cisa.gov/national-cybersecurity-communications-integration-center).

[12] Digital Forensics Research Workshop (DFRWS), Trumansburg, NY (dfrws.org), 2020.

[13] Forum of Incident Response and Security Teams (FIRST), CSIRT Framework Development SIG, Cary, North Carolina (www.first.org/global/sigs/csirt/).

[14] Forum of Incident Response and Security Teams (FIRST), FIRST is the global Forum of Incident Response and Security Teams, Cary, North Carolina (www.first.org).

[15] S. L. Garfinkel, Digital forensics research: The next 10 years, *Digital Investigation*, vol. 7, pp. S64–S73, 2010.

[16] Global Resilience Institute at Northeastern University, Cyber NTSB (globalresilience.northeastern.edu/research/cyber-ntsb/).

[17] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Idaho Falls, Idaho (www.us-cert.gov/ics).

[18] H. Krawczyk, M. Bellare and R. Canetti, HMAC: Keyed-Hashing for Message Authentication, RFC 2104, Internet Engineering Task Force, 1997.

[19] LANGSEC, LANGSEC: Language-theoretic Security (langsec.org/).

[20] Linux Foundation, The Update Framework (TUF): A framework for securing software update systems (theupdateframework.github.io).

[21] Linux Foundation, Uptane: Securing Software Updates for Automobiles, Linux Foundation (uptane.github.io/).

[22] M. Locasto, M. Burnside and D. Bethea, Pushing boulders uphill: The difficulty of network intrusion recovery, *Proceedings of the Twenty-Third Large Installation System Administration Conference*, 2009.

[23] R. McQuaid, R. Graubart and D. Bodeau, Designing for Resilience, *The MITRE Corporation* (www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/designing-for-resilience), July 24, 2017.

[24] National Transportation Safety Board, About the National Transportation Safety Board, Washington, DC (www.ntsb.gov/about/pages/default.aspx).

[25] National Transportation Safety Board, Aviation Accident Reports, Washington, DC (www.ntsb.gov/investigations/AccidentReports/Pages/aviation.aspx).

[26] National Transportation Safety Board, Cockpit Voice Recorders (CVR) and Flight Data Recorders (FDR), Washington, DC (www.ntsb.gov/news/pages/cvr_fdr.aspx).

[27] National Transportation Safety Board, The Investigative Process, Washington, DC (www.ntsb.gov/investigations/process/Pages/default.aspx).

[28] National Transportation Safety Board, Safety Recommendation Report: Extended Duration Cockpit Voice Recorders, ASR1804, Washington, DC, 2018.

[29] L. Nolan, Practical Incident Response, presented at *SRECon16 Europe* (www.usenix.org/conference/srecon16europe/program/presentation/nolan), 2016.

[30] QED Secure Solutions, Risk Scoring System For Aviation Systems, Coppell, Texas (www.riskscoringsystem.com/aviation/).

[31] N. Robinson, The Case for a Cyber-Security Safety Board: A Global View on Risk, *The RAND Blog* (www.rand.org/blog/2012/06/the-case-for-a-cyber-security-safety-board-a-global.html), June 18, 2012.

[32] P. Rosenzweig, The NTSB as a Model for Cybersecurity, R Street Institute, Washington, DC (2o9ub0417chl2lg6m43em6psi2i-wpengine.netdna-ssl.com/wp-content/uploads/2018/05/Final-Short-No.-58.pdf), 2018.

[33] R. Sabatini, Cyber security in the aviation context, *Proceedings of the First Cyber Security Workshop*, 2016.

[34] S. Shackelford. The U.S. Needs an NTSB for Cyberattacks, *Wall Street Journal* (`www.ntsb.gov/news/pages/cvr_fdr.aspx`), June 4, 2019.

[35] The MITRE Corporation, Common Vulnerabilities and Exposures (CVE), Bedford, MA (`cve.mitre.org`).

[36] Trusted Computing Group, Trusted Platform Module (TPM) Summary, Beaverton, Oregon, USA (`trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/`), 2008.

[37] U.S. Computer Emergency Readiness Team (US-CERT), Washington, DC (`www.us-cert.gov/`).

[38] Wikipedia Contributors, ARINC 429 *Wikipedia Commons*, (`https://en.wikipedia.org/wiki/ARINC_429`).

[39] Wikipedia Contributors, Digital Forensics (`en.wikipedia.org/wiki/Digital_forensics`).