

FAA Aviation Mx Human Factors Quarterly



September 2021
Vol 9, Issue 3

Inside This Issue

How Safety-Critical Businesses Can Improve Cybersecurity Risk Management

Marc Szezan

Page 3

Proposes five steps that aviation and other safety-critical business can consider to integrate cybersecurity considerations into safety management thinking along their global supply chains.

Following SOP Ensures Safe Operations

P.S. Ganapathy

Page 7

Reminder of the importance of following Standard Operating Procedures (SOP).

How to Present Human Factors in a “Snap Shot”

Bill Johnson

Page 8

Provides suggestions for preparing a “Snap Shot” for use in advocating the management of human factors hazards.

If you would like to subscribe, please click on the following link [Subscribe](#).

The views and opinions expressed in this quarterly forum are those of the authors and do not necessarily reflect the official policy or position of the FAA, editor, or quarterly forum staff.

Upcoming Events

Do you know of an event that you would like us to share?

Send information to Janine King Janine.CTR.King@faa.gov or Dr. Kylie Key Kylie.N.Key@faa.gov.

Editor's Note: These events may have been cancelled or postponed due to the ongoing pandemic. Please consult the event website for confirmation before planning to attend these events.

- Pacific Airshow
[Huntington Beach, CA \(October 1-3, 2021\)](#)
- MRO Europe
[Amsterdam, The Netherlands \(October 19-21, 2021\)](#)
- INFO Share Conference 2021
[Gdańsk, Poland \(Oct 14-15, 2021\)](#)
- Aerospace Incubator
[Miami, FL \(November 1-4, 2021\)](#)
- AVALON 2021 – Aerospace & Defense Exposition
[Victoria, Australia \(November 23-28, 2021\)](#)



We're Taking Submissions

Want to share an article or experience in an issue of the FAA Aviation Mx HF Quarterly?

The Mx HF Quarterly is published every 3 months, beginning at the end of March. We welcome your articles related to aviation maintenance. Our great editorial team will review submissions to ensure that content and format meet the needs of our readers. Editorial feedback is subject to author approval prior to the publication.

Please include the following with your submission

- Short author biography (50-150 words)
- Photo of yourself for biography
- One-sentence summary of your article
- Images and/or graphics (with captions)
- Call-out quote(s)
- Takeaway message (what you hope the readers takeaway) from your article (not to exceed 100 words)

Send your submissions to Janine King at Janine.CTR.King@faa.gov.

Author Appreciation

We, the editorial team, extend our gratitude to our readers and contributors for their continued support of this quarterly publication. Our contributors and authors are not primarily responsible for writing articles for this quarterly newsletter; however, their vast knowledge and understanding of issues influencing and relating to aviation maintenance substantially improve this publication.

If you are interested in providing suggestions or feedback concerning this publication, or would like to submit an article or notify us of an upcoming event, please email Janine King at Janine.CTR.King@faa.gov or Dr. Kylie Key at Kylie.N.Key@faa.gov.

We look forward to not only new article submissions but to reviews and feedback from our readers.

We appreciate your input!

How Safety-Critical Businesses Can Improve Cybersecurity Risk Management

Marc Szepan

Safety management in aviation puts a strong emphasis on management of organization-internal risks. However, aviation businesses neglect organization-external risks at their own peril. Given the realities of an increasingly digitized world, cyber threats rank amongst the most consequential of these organization-external risks. Aviation and other safety-critical businesses would be well-advised to take a holistic approach to safety management and to integrate cybersecurity considerations into safety management thinking. This article proposes five steps that safety-critical organizations such as airline maintenance & engineering operations or repair stations can consider to improve their cybersecurity risk management.

Global Cyber Threat Reality

Since the beginning of 2021, a number of high-profile cyberattacks in and outside the aviation industry have been in the news. For example, in early 2021, SITA experienced a breach of its servers resulting in significant leakage of air passenger data. In May, Colonial Pipeline, a key building block of the U.S. energy system, became target of a ransomware attack that disrupted gas deliveries along the U.S. East Coast. In July, Kaseya, a provider of IT and security management solutions, fell victim to a ransomware attack that affected businesses around the world.

These examples are just the visible tip of a much larger cyber threat iceberg. Global cyber threats have proven to be extraordinarily costly. A recent McAfee report, *The Hidden Costs of Cybercrime*, estimates the total worldwide monetary loss from cybercrime at approximately US\$ 945 billion in 2020 alone. Cybersecurity has been one of the top-of-agenda concerns for leaders of public, private, and civic sector entities for some time. It is no surprise that the most recent edition of the Allianz Risk Barometer ranks



cyber incidents among the Top 3 global business risks for 2021.

***“IN THE CASE OF AVIATION AND OTHER
SAFETY-CRITICAL BUSINESSES, CYBER
THREATS CAN EASILY TRANSLATE INTO
FUNDAMENTAL SAFETY RISKS.”***

Cyber Risks in Aviation

Many, if not most, of the aforementioned cyberattacks have resulted in significant costs for affected corporate targets. However, many of these costs have “only” been of a financial, continuity-of-business, loss-of-

intellectual-property, customer satisfaction or reputational nature.

Five Steps to Improve Cybersecurity

1. Prioritize target and maintain radar lock!

2. Build cybersecurity capability and capacity!

3. Ensure situational awareness!

4. Put in place or fine-tune a Cybersecurity Management System!

5. Cover entire global supply chain!

© Marc Szepan, 2021

In contrast, in the case of aviation and other safety-critical businesses, cyber threats can easily translate into fundamental safety risks. In the specific case of airline maintenance & engineering operations and repair stations, cyber vulnerabilities exist in a number of safety-relevant areas. For example, scheduling of maintenance actions is critically contingent upon reliability of Maintenance Schedules, accurate tracking of individual life-limited parts, and availability of correct aircraft utilization data. Proper performance of specific maintenance tasks is dependent on completeness and up-to-date-ness of such documents as Maintenance Task Cards, Aircraft Maintenance Manuals, and Structural Repair Manuals. Usage of tooling is subject to compliance with calibration standards and intervals. Data compromise or alteration in any of these areas due to a cyberattack, targeted or otherwise, could fundamentally impact safe maintenance operations.

Also, cyber risks in aviation are particularly pronounced due to often globally distributed airline operations and

“GIVEN THAT CYBER THREATS CAN RESULT IN FUNDAMENTAL SAFETY RISKS AND REGULATORY NON-COMPLIANCE AS MUCH AS IN FINANCIAL AND OTHER TYPES OF DAMAGE, LEADERS OF SAFETY-CRITICAL AVIATION BUSINESSES WOULD BE WELL ADVISED TO PUT CYBERSECURITY ON THE TOP OF THEIR AGENDA.”

the multi-party nature of aviation supply chains.

Five Steps to Improve Cybersecurity

Given that cyber threats can result in fundamental safety risks and regulatory non-compliance as much as in financial and other types of damage, leaders of safety-critical aviation businesses would be well advised to put cybersecurity on the top of their agenda. The following five steps are intended to be a helpful guide to ensure that cybersecurity considerations are integrated into safety management thinking:

1. Prioritize target and maintain radar lock!

Sometimes, cybersecurity is viewed as a “techy” issue and as primary responsibility of the IT group. Both of these views are unhelpful at best and potentially dangerous at worst. Managing cyber risks is as much a matter of utilizing the right type of IT tools as it is of putting in place and sustaining the right type of cyber risk-aware culture, organizational design, process architecture, and human resources. Given this holistic approach to cybersecurity, by definition, lead responsibility rests with the senior leadership team of a business and not just with its IT group. Senior leadership needs to anchor cybersecurity as a top-of-agenda strategic priority and needs to maintain continuous focus on cybersecurity-related issues, including in the context of safety management.

2. Build cybersecurity capability and capacity! As cybersecurity should not be delegated to the IT group and should be approached as an enterprise-wide effort, appropriately calibrated cybersecurity expertise should be built within an airline maintenance & engineering operation or a repair station. These efforts should not duplicate IT-specific “techy” expertise. Instead, they should complement IT-specific know-how to ensure that considerations in non-IT expertise domains such as human behavior, organizational design, process architecture, aviation-specific technology, and regulatory requirements are adequately championed in the interest of a balanced approach to managing cyber risks. Building this cybersecurity expertise outside IT groups requires sufficiency in budget allocation and HR headcount resourcing.

3. Ensure situational awareness! Once enterprise-wide cybersecurity expertise has been put into place, aviation businesses need to develop a realistic understanding of their potential cyber vulnerabilities and the degree of their readiness for identifying, analyzing, and eliminating or mitigating cyber risks. In order to develop this situational awareness, an enterprise-wide cybersecurity audit should be conducted, possibly with external support. Similar to safety management audits, cybersecurity audits should be comprehensive, in-depth, and no-holds-barred. In the spirit of a balanced approach to managing cyber risks, cybersecurity audits should not only be focused on IT-specific “techy” issues. They should cover all aspects of cybersecurity. A good cybersecurity audit identifies specific cyber vulnerabilities and inadequate defenses and results in actionable recommendations.

4. Put in place or fine-tune a Cybersecurity Management System!

In accordance with U.S. Cybersecurity & Infrastructure Security Agency (CISA) standards, cybersecurity addresses the protection of networks, devices, and data from unauthorized access or criminal use. It ensures confidentiality, integrity, and availability of data. Similar to managing safety risks, managing cyber risks is a function of systematic and formal identification, assessment, and elimination or mitigation relative to defined acceptable risk levels. On the basis of a completed enterprise-wide cybersecurity audit, aviation businesses can build from scratch or fine-tune existing Cybersecurity Management Systems within the context of a cyber-risk level that they are willing to incur while, at a minimum, ensuring regulatory compliance. When developing Cybersecurity Management Systems, aviation businesses would be well advised to leverage state-of-the-art technology and, at the same time, to not forget basic common sense. For example, CISA basic cybersecurity best practices include keeping software up-to-date, running up-to-date antivirus

***“IN AN INCREASINGLY DIGITIZED WORLD,
CYBER THREATS ARE ONE OF THE MOST
CONSEQUENTIAL RISKS FOR ANY BUSINESS.”***

software, implementing multi-factor authentication (MFA), and installing firewalls. A good Cybersecurity Management System also includes contingency plans for responding to cyberattacks and regular response simulations, including a business' senior management team.

5. Cover the entire global supply chain! As mentioned above, cyber risks in aviation are often exacerbated by the globally distributed and multi-party nature of supply chains. A particular airline maintenance &

engineering operation or aviation repair station might well have put in place a state-of-the-art Cybersecurity Management System at its home base. Still, significant cyber vulnerabilities are likely to remain if an airline's (outsourced) international line maintenance operations or a repair station's global supply chain are not covered by the same cybersecurity standards as its home base operations. Aviation businesses need to ensure that their Cybersecurity Management System covers all global supply chain partners and vendors in all venues.

Closing Thoughts

In an increasingly digitized world, cyber threats are one of the most consequential risks for any business. Aviation and other safety-critical businesses should take a holistic approach to safety management that addresses both organizational-internal risks and organization-external risks such as cybersecurity. A well-configured Cybersecurity Management System should be predicated on a balanced approach that does justice as much to IT "techy" issues as to non-IT risk factors. This article proposes five steps that safety-critical organizations such as airline maintenance & engineering operations or repair stations can consider to integrate cybersecurity considerations into their safety management thinking along their entire global supply chains.

TAKEAWAY MESSAGE

In an increasingly digitized world, cyber threats are one of the most consequential risks for any business. Aviation and other safety-critical businesses would be well-advised to take a holistic approach to safety management that integrates cybersecurity considerations into their safety management thinking. A well-configured Cybersecurity Management System should be predicated on a balanced approach that does justice as much to IT "techy" issues as to non-IT risk factors. There are five steps that can be considered to improve cybersecurity along global supply chains.

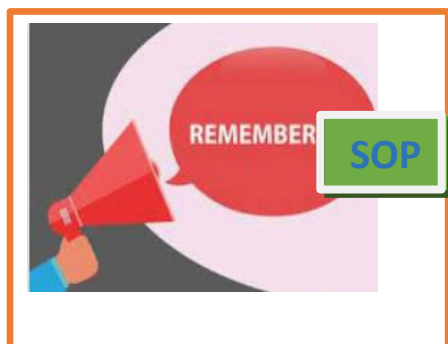
Dr. Marc Szepan is a Lecturer in International Business at the University of Oxford Saïd Business School. Previously, he was an executive at Lufthansa. In 2012, Marc was recognized as one of Aviation Week & Space Technology's "40 Under Forty: Rising Stars of Aerospace and Aviation".



Following SOP Ensures Safe Operations

Safety Slogan – August, 2021

P.S. Ganapathy



The author has regularly prepared a safety slogan since 2019, distributable to various aviation groups and organizations. This content is a reprint of content prepared as the August 2021 Safety Slogan, titled "Following SOP ensures Safe Operations". The author used numerology to support the message that following SOPs ensures safe operations. The interested reader may contact the author for additional details at psganapathy42@gmail.com.

Standard Operating Procedures (SOP)

Facilitate mastering actions for reducing errors

Outline operating philosophy of what to do and when to do

Live document providing directions

Lessen ambiguities and error risks

Offer job steps that help standardization

Written procedures for performance of tasks

Set of rules guaranteeing efficiency and consistency

Organization's powerful safety and quality tool

Provides assurance for better task sharing

SOP is meant to achieve
Safe
Outstanding
Performance

REMEMBER that pilots who **deviate**
from SOPs are **three times more likely**
to commit errors and **that half of all**
CFIT accidents involve failure to
adhere to them.

Passionately FOLLOW SOP and AVOID Normalizing Deviations

P.S. Ganapathy, M.Sc and Ae.S.I is currently a senior aviation consultant with over 50 years of flight operations experience in Airlines and Aviation organization. Retired as a General Manager -Flight operations, Air India after 33 years. Later worked in the capacity of Aviation Consultant and Manger Regulatory Compliance, CRM Facilitator in Oman Air and Directorate of Police Aviation, Royal Oman Police in MUSCAT for 13 years. Now presently conducting training to Aviation organizations' pilots, engineers and ground staff on Human Factors and SMS on need basis.



How to Present Human Factors in a “Snap Shot”

Bill Johnson

Dr. Bill recently taught a segment of a Safety Management System course in cooperation with a team of professionals from the Department of Transportation Safety Institute (TSI). His session was entitled “Considering Human Factors (HF) in Safety Management Systems (SMS).” The topic was critical because human factors issues are among the most prevalent of aviation safety risks. These issues contribute to about 80% of all negative events, therefore necessitating management within the context of Safety Management Systems.

The 40 participants in the weeklong class were FAA employees from the Flight Standards and Aircraft Certification organizations whose primary responsibility within the FAA relates to SMS oversight. Participants were experienced in aviation with an average of 35 years in aviation and an average of three aviation employers prior to the FAA. With such an experienced group, you would suspect that all would have received human factors training, but you would be wrong. While some participants had “More than they could count,” others indicated no prior human factors training.

FAA Aviation Safety Inspectors and industry SMS implementers should be able to discuss the importance of human factors in SMS oversight. As front-line advocates of SMS, it is our role to communicate the *Why* and *How* of managing human factors. It is important that we are able to communicate a clear and high value, applications-oriented, human-centered safety message at a moment’s notice.

When it comes to presenting human factors, there is no such thing as “one size fits all.” It is best to tailor your message to the audience, and the experience and comfort level of the speaker. This article offers suggestions for content and delivery suggestion to help you build a human factors “Snap Shot” that works for you and your audiences.

Delivery Suggestions

Be Clear

Your goal is to deliver a clear message that will enhance your audience’s ability to understand, appreciate, and apply human factors to their work. Your audience may oversee SMS implementation but they may also be aviators who fly, maintain aircraft, or oversee flight safety. To ensure that your message is useful and applicable to diverse audiences, deliver organized, simple concepts in plain language.

Deliver a Good Story

Consider your snap shot to be a story. Grab attention with an example or event. Explain how human factors played a role in the event. Use pictures and slides to illustrate your story. To promote retention, bullet or call the takeaway messages for your audience. Know your story and avoid falling back on reading your slides or embedded notes. Most importantly, make the story your own. For suggestions on how to tell your story, see [Story Telling Tips – How to Improve Your Hangar Talk and War Stories](#)¹.

**“FAA AVIATION SAFETY
INSPECTORS AND INDUSTRY SMS
IMPLEMENTERS SHOULD BE ABLE
TO DISCUSS THE IMPORTANCE OF
HUMAN FACTORS IN SMS
OVERSIGHT.”**



Content Suggestions

Event and Accident Scenarios where Human Factors Contributed

One effective way to provide tangible content is to illustrate human factors contributors to accidents and other negative safety events. Following are suggestions for selecting events as good examples for your story, where to find event narratives, and a readymade compilation of events. For tips on using events as a way to teach human factors, see [PEAR Model Approach in Applying Human Factors to Enhance Aviation Safety](#)².

Selecting event(s): The best examples of events are those that are very familiar to you. If applicable, talk about your own human factors errors as a pilot or mechanic to provide credibility with your audience. Remember that when selecting examples, they don't need to be "Big" accident(s) to make a solid point. Non-fatal events are can be good candidates for discussion. Remember that if fatalities were involved, it is critical to acknowledge the gravity of the human losses.

Event examples: Summaries and descriptions of events and accidents are available online via databases such as Corporate Aviation Safety Action Program (ASAP) databases, the Aviation Safety Information and Sharing (ASIAS) database, or the National Transportation Safety Board (NTSB). Although these databases are loaded with high-value reports, they contain confidential information and may not include sufficient publicly available detail to enhance your story.

Another source is the DOT Transportation Safety Institute 'HF in Aviation Maintenance' course, which provides a series of event examples. See the list below and the associated official reports.

Links to HF-Related Events

- [B787 Gear Pin Instillation](#) (Multiple events)
- [B747 Landing Gear Actuator](#) (December, 2014)
- [AS365 N3 Helicopter Flight Controls](#) (June, 2020)
- [AS350 B2, Flight Controls](#) (December, 2011)
- [B737 Max 8](#) (2018, 2019)

General Ways to Consider Human Factors

A human factors model may help you look at historical events or work environments to evaluate human factors hazards. The three most [popular HF models](#) are PEAR, Dirty Dozen, and Swiss Cheese. For a discussion on applying these models to SMS, see Aviation Pros [Trusted Human Factors Sources](#).

***"LOOK AT THE FAA MAINTENANCE HUMAN FACTORS WEBSITE AND THE
FAA SAFETY TEAM SITE (FAASAFETY.GOV) FOR TRAINING AND SUPPORT
MATERIALS."***

Offer the Most Common Human Factors Contributors, Using FAA Resources

The most common human factors-related contributing factors to an event are neither a secret nor a surprise. The three top contributing factors in aviation maintenance are: 1) safety culture and leadership; 2) procedural noncompliance; and 3) fitness for duty. The FAA Human Factors in Aviation Maintenance website (www.humanfactorsinfo.com) supports the goal of identifying and optimizing the factors that affect human performance in maintenance and inspection and has sections dedicated to fatigue and to procedural compliance.

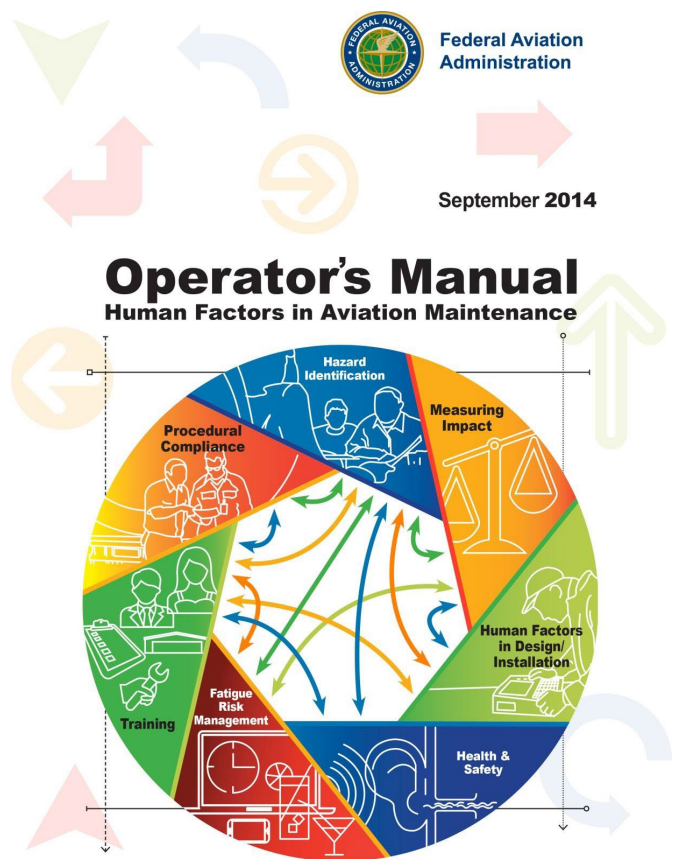
A sampling of the available resources include:

- [Training course](#) promoting a culture of procedural compliance
- Fatigue awareness campaign materials, including signage and the 18-minute video, “[Grounded](#)”
- [The Operator’s Manual for Human Factors in Maintenance](#)³

As you consider the best content for your snap shot, look at the FAA Maintenance Human Factors website and the FAA Safety Team site (faasafety.gov) for training and support materials.

Wrapping Up

FAA Aviation Safety Inspectors and SMS Implementation gurus must advocate the importance of considering human factors within the context of SMS. By having a human factors *Snap Shot* prepared, you will be better poised to advocate at a moment’s notice. I hope the tips provided herein will help you build a human factors *Snap Shot* that works for you and your audiences.



TAKEAWAY MESSAGE

Because human factors are included in around 80% of all negative safety events, FAA Aviation Safety Inspectors and SMS Implementation experts must advocate the importance of human factors. This article provided suggestions for developing a human factors *Snap Shot* designed to deliver a good story with a clear message conveying the importance of managing human factors in Safety Management Systems (SMS). The tips provided will help maximize the value of preparing a human factors *Snap Shot* presentation so that key stakeholders are prepared at a moment’s notice to advocate for human factors risk management.

References

1. Johnson, W.B. (2016). Story Telling Tips – How to Improve Your Hangar Talk and War Stories. *Aircraft Maintenance Technology Magazine*. Oct. 2016, pp. 58-61. <https://www.aviationpros.com/tools-equipment/insurance-finance/aircraft/article/12250848/storytelling-tips-how-to-improve-your-hangar-talk-and-war-stories>
2. Johnson, W.B. (2016). PEAR Model Approach in Applying Human Factors to Enhance Aviation Safety. *Journal of Aviation Management*, Singapore: Singapore Aviation Academy. Fall, 2016, pp. 19-28. https://saa.caas.gov.sg/documents/35058/35139/SAA_Journal_2016.pdf/3913c788-5340-7a6a-d9e2-5626b369d749?t=1606990986875

3. Johnson, W.B. & Avers, K.A. (Eds.) (2014). *The Operator's Manual for Human Factors in Aviation Maintenance*. Washington, DC: Federal Aviation Administration. (See www.humanfactorsinfo.com)

Dr. Bill Johnson, a frequent contributor to this newsletter, is the former FAA Chief Scientific and Technical Advisor for Human Factors in Aircraft Maintenance Systems. His comments are based on nearly 50 years of combined experience as a pilot, mechanic, airline engineering and MRO consultant, a professor, an FAA scientific executive, and now President and Chief Scientist for Drbillj.com LLC.



Other HF Resources and Links

Click the icon for more information

Follow Procedures: The Buck Stops with Me



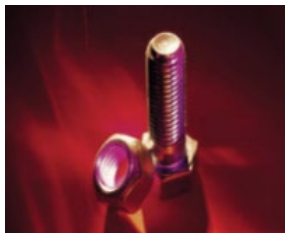
FAA Training Tools and Resources



Aviation Human Factors Industry News by System-Safety.com



Nuts and Bolts Newsletter



Aviation Maintenance



ICAO Journal



FAA and Industry General Aviation Awards



FAA Mechanic Award Programs

Mechanic Award Programs

Aircraft Maintenance Technology

