Critical Systems Labs
Strategic Insight for Safety

Integration of Security and Airworthiness in the Context of Certification and Standardization

Laurent Fabre and Jeff Joyce
Critical Systems Labs
jeff.joyce@cslabs.com

SafeComp 2014 – ISSE workshop
8 September 2014

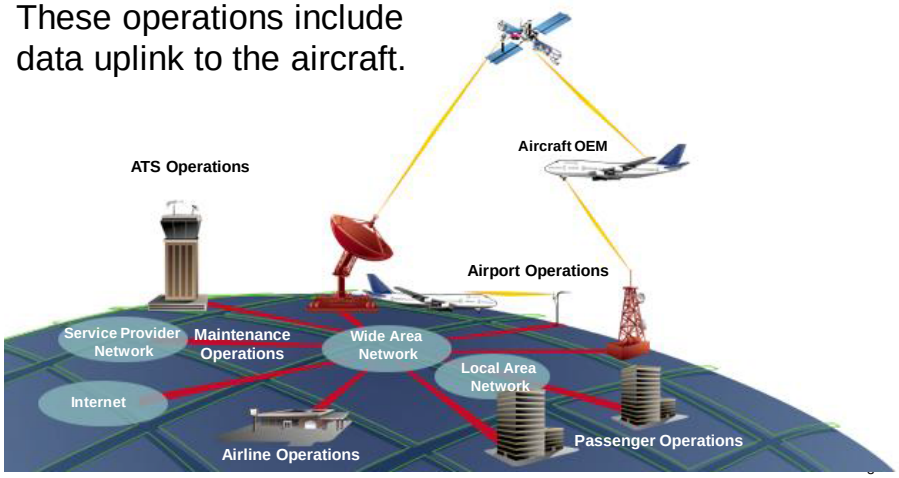
Introduction

- This presentation covers:
  - How the aerospace community has addressed the challenges of integrating safety and security through guidance in recently published standards
  - Fundamental questions that have been prompted by this work such as the impact of security on safety
- Aerospace practices and standards have often influenced other industries, could this model be a good model for other industries too?

Critical Systems Labs
Strategic Insight for Safety

Aircraft are highly connected

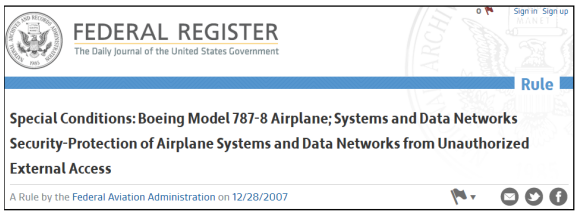
The aircraft becomes another node available for network-centric operations.
These operations include data uplink to the aircraft.



Critical Systems Labs
Strategic Insight for Safety

Cyber-security Certification context

- Aircraft type certification acts in the absence of comprehensive rules and guidance for how cyber-security affects safety
- FAA, Transport Canada and EASA used an ad-hoc process in the form of 'Special Conditions' to address specific security concerns for specific aircraft model


FEDERAL REGISTER
The Daily Journal of the United States Government

Rule

Special Conditions: Boeing Model 787-8 Airplane; Systems and Data Networks Security-Protection of Airplane Systems and Data Networks from Unauthorized External Access

A Rule by the Federal Aviation Administration on 12/28/2007

RTCA SC-216
Aeronautical Systems Security

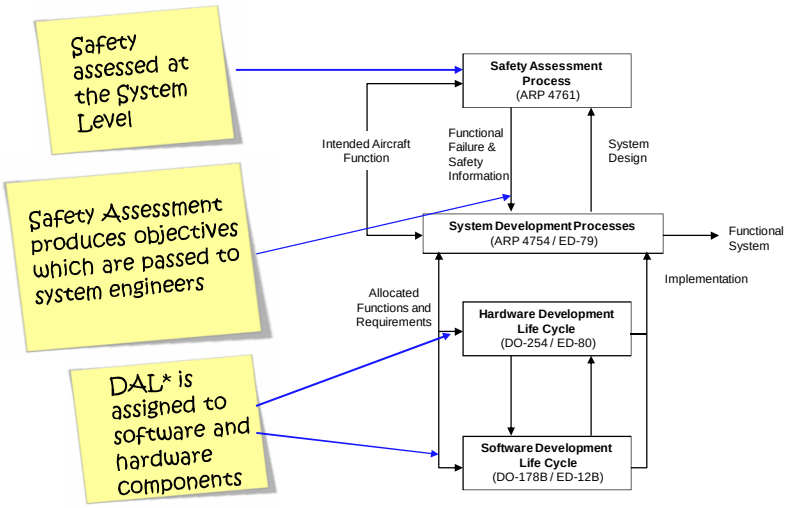
- Special Committee formed in June 2006
- Collaborative work with EUROCAE WG-72
- 2014 achievements:
  - Released two new documents and expects to release a third one in the fall
  - Consistent set of documents in terms of terminology, scope and guidance
  - Anticipated to become reference documents for the certification of aircraft and aircraft systems in the context of information security

A set of three consistent standards

Document	Title		Publication date
DO-326A / ED-202A	**Airworthiness Security Process Specification**	The process document proposes guidance to assess security risk, design security protection and ensure effectiveness of these protections **The What part**	August 2014
DO-YY3*	**Airworthiness Security Methods and Considerations**	This document provides considerations and methods to support the process and the activities described in DO-326A. **The How part**	Expected September 2014
DO-355 / ED-204	**Information Security Guidance for Continuing Airworthiness**	This document proposes guidance to develop Instructions for Continued Airworthiness (ICA) and guidance for the operation and maintenance of aircraft and for organizations and personnel involved in these tasks .	June 2014

* No EUROCAE counterpart, at least initially

Safety Assessment in the aerospace world



*Development Assurance Level, equivalent to SIL in other industries

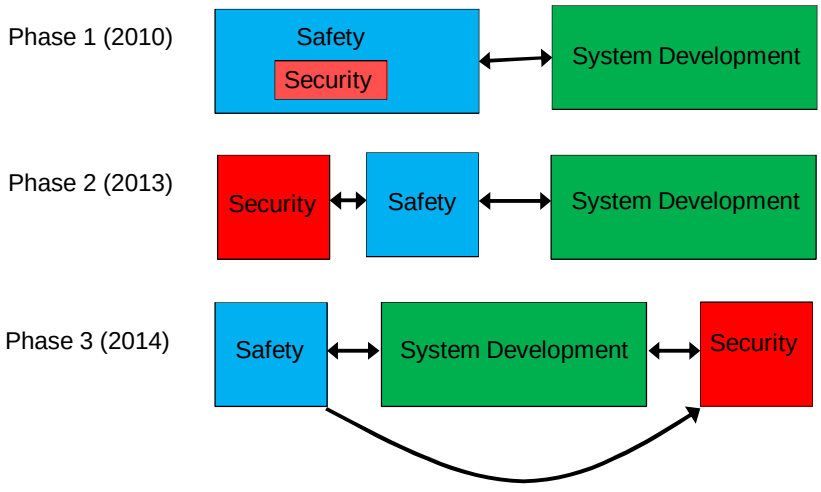
Security activities vs Safety activities

- A recurring topic for this special committee was to address the relationship between security and safety activities. In particular does the security assessment fall under the umbrella of the safety assessment?
- As DO-326 evolved, the relationship between security and safety went from a tight integration of activities to a clear demarcation with some defined interactions

Security activities vs Safety activities

- In the 2010 standard, the security activities were depicted as embedded within the safety activity
  - The safety FHA was seen as including threat conditions along with failure conditions.
  - The certification authorities liked this approach because it makes it easier to have a combined picture of risks to the safety of flight
- In the draft versions of the A standard, security activities were extracted from the safety activities and positioned parallel to the safety activities
- In the final version of 326A, security activities are no longer positioned next to the safety activities. System activities have been inserted between them

Phase 1, 2 and 3 (DO-326A):

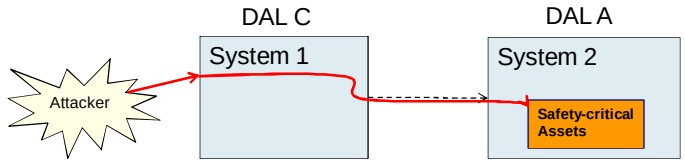


Rationale for the segregation of safety and security activities

- However 326A does not prevent an airframer from allowing security information to flow directly to safety (e.g., threat conditions being consolidated into the Functional Hazard Analysis) -- airframers can do this if they wish. But it's not mandated by DO-326A.

Impact of Security Risk on DAL (1 / 4)

- Another important topic deals with the impact of the security risk assessment to the system and to the allocation of the Development Assurance Level (DAL)?
- How does security risk assessment affect the determination of the DAL? Is it possible that the DAL associated with some software function might be higher as a result of considering security vulnerabilities than it would otherwise have been if only failure conditions had been considered?



Should System 1 DAL be increased?

Impact of Security Risk on DAL (2 / 4)

- Theories:
  - Theory #1: no impact. If one claims that there is an impact, it means that the initial safety assessment overlooked some interfaces that carry important information and may not be complete
    - ➔ Safety assessment should be re-visited
  - Theory #2: "Of course" there could be an impact to the DAL. There will be specific cases where the DAL needs to be increased because of security concerns. (this is the stated position in the Consideration and Methods document: DO-YY3 publication imminent)

Impact of Security Risk on DAL (3 / 4)

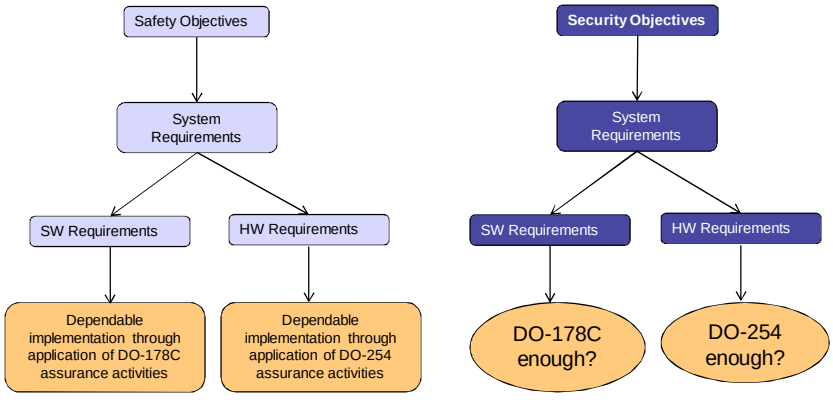
- Theory #3: no impact to the DAL because the DAL should be left alone. However the security risk needs to be addressed by a different level scheme i.e. a Security Level (SL) or Effectiveness Assurance Level (EAL) (EUROCAE approach)

A set of assurance activities will be assigned to each SL or EAL with different expectations regarding thoroughness and rigor

Impact of Security Risk on DAL (4 / 4)

- Related considerations
  - Should keep in mind that an aircraft OEM needs to present a consolidated picture to certification authorities so keeping two different assurance levels (the DAL + security assurance level) might be confusing.
  - Practically it will be difficult to increase the DAL of a flight control systems that has been implemented at a certain level for several generations of aircrafts. In general, the designers will add an architectural mitigation as a justification to keep the original system DAL (before security consideration)

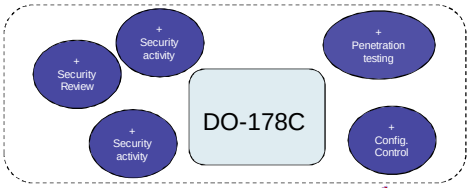
Assurance activities for Security (1/2)



- A safe system relies on a dependable implementation of the software/hardware through the application of assurance activities as specified by DO-178C / DO-254
- Which assurance activities are required for Security?

Assurance activities for Security (2/2)

- Group consensus: additional activities e.g., independent review, penetration testing are needed for the sake of security, but no consensus on the list of such activities, the specification of these activities and the level to which they have to be performed.
  - DO-YY3 suggests a set of ad-hoc supplemental activities. The rigor and depth of these activities is not specified.



  - EUROCAE WG seemingly advocat… …rity level scheme that more systematically identifies wha… …tivities are needed according to security risk assessm… …view may be somewhat influenced by common criteria).

Under development

Conclusion

- Three standards focused on Airworthiness Security Guidance published in 2014:
  - DO-326A / ED-202A
  - DO-YY3 (expected publication Sep-Oct 2014)
  - DO-355 / ED-204
- After several iterations, the published version of DO-326A depicts Safety and Security activities as de-coupled despite the expressed preference of some regulation authorities. System-level activities bridge safety and security outcomes.
- The influence of security assessment on the DAL is a contentious topic. No clear consensus within the community about the answer.