Safety and Security – Can they Coexist?

Scott Engle

Director of Business Development and Capture

Embedded Tech Trends

January 29, 2019

Safety and Security are ***not*** mutually exclusive

For safety-critical systems to be truly safe, they must also include security

What do we mean by a “safe” system?

- Systems developed under a requirements-driven safety process
  - Examples include DO-254 and DO-178C for avionics
  - IEC 61508 for industrial, ISO 26262 for automotive
- Follow typical V-Shaped development process
- Process involves verification and validation activities, documents

A mature process making flying one of the safest modes of transportation

What do we mean by “security”?

- Generally refers to two areas: Cyber Security and Anti-Tamper
- Cyber Security: Practice of protecting systems from digital attacks
  - Protecting assets as well as data
- Security has guidelines vs. requirements
- Common method to protect device is to reduce ‘entry points’ or isolate system completely…

…and to protect against attack through the entire lifecycle

Security concerns dominated by fear and hype

- Must dismiss FUD that security incidents/Hollywood create
- Chris Roberts didn't hack into Thrust Management System through In-Flight Entertainment System
- Aircraft companies and nuclear power plant designers will continue to keep safety-critical systems and guest Wi-Fi access points separate
- This does not mean vulnerabilities do not exist

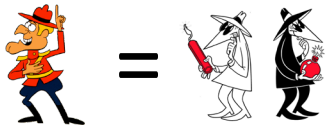
Efforts to thwart Cyber attacks should be based on realistic threats

Ecosystems are becoming increasingly connected

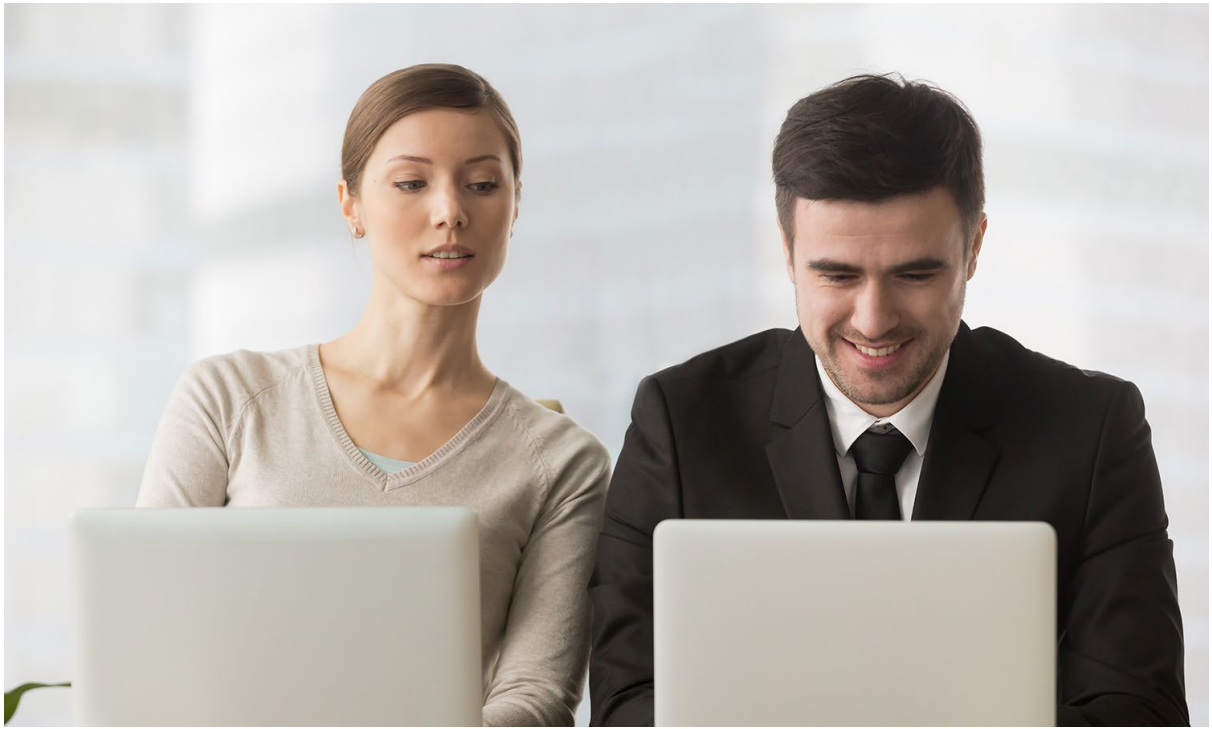
- Systems becoming more connected; aircraft, automobiles, trains, etc.
- IoT revolution has brought cost savings by making devices smarter and more manageable… but at a cost
- We are becoming more reliant and dependent on connectivity
- Over 150,000 incidents of GPS jamming or interference in past 3 yrs
  - Pokemon Go app encouraged hackers to spoof GPS to win prizes
- Hackers only have to be right once!

Many more ways in which bad actors can gain access to systems

Where safety and security are similar

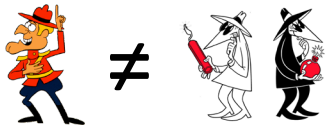


- Both benefit from strong requirements-driven process…
- … and from monitoring of critical functions/interfaces
- ‘Spousal Circuitry’: Monitors critical interfaces for unusual activity; alerts appropriate operator
- Hackers generally take advantage of defects; so do mishaps
- Reducing attack surfaces
- Figure out ways to break system and keep that from happening
- Simple designs have greatest chance of success



Safety and security have a lot more in common than we think

Where safety and security are different



- Security is continually evolving; Safety is static
- New security threats, ever increasing sophistication of attacks
  - Updates to security are routine
  - Updates to safety only if absolutely necessary
- If a function is safety-critical it cannot be disabled or halted
  - In security if compromise is detected, interface can be disabled
- Testing for safety and for security completely different disciplines

Safety functions must continue to operate without exception

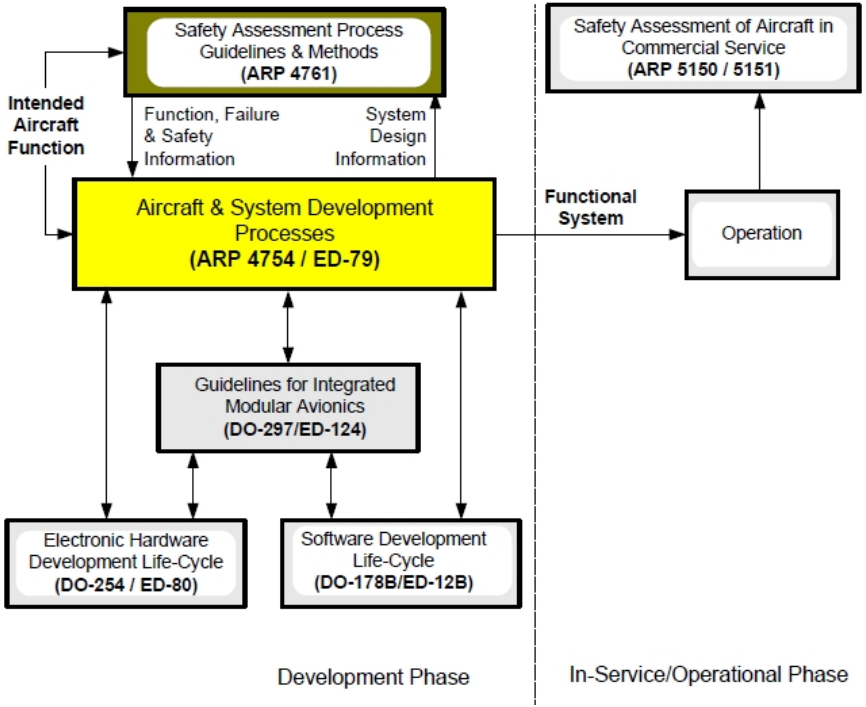
Where to start?

- Certification authorities expect that applications have safety foundation
  - Systems start secure (trusted boot and load signed images)
  - Security gives way to safety except for security monitoring of critical interfaces
- More cost-effective to add security to system that is already certified safe
  - vs. adding safety to a system that has already been proven secure
- Where to inject security requirements into the current safety process?
  - Should be added at system/functional level
- Ideally both features should be requirements from the beginning

Start safe, become secure

Adding security to safety at the functional level

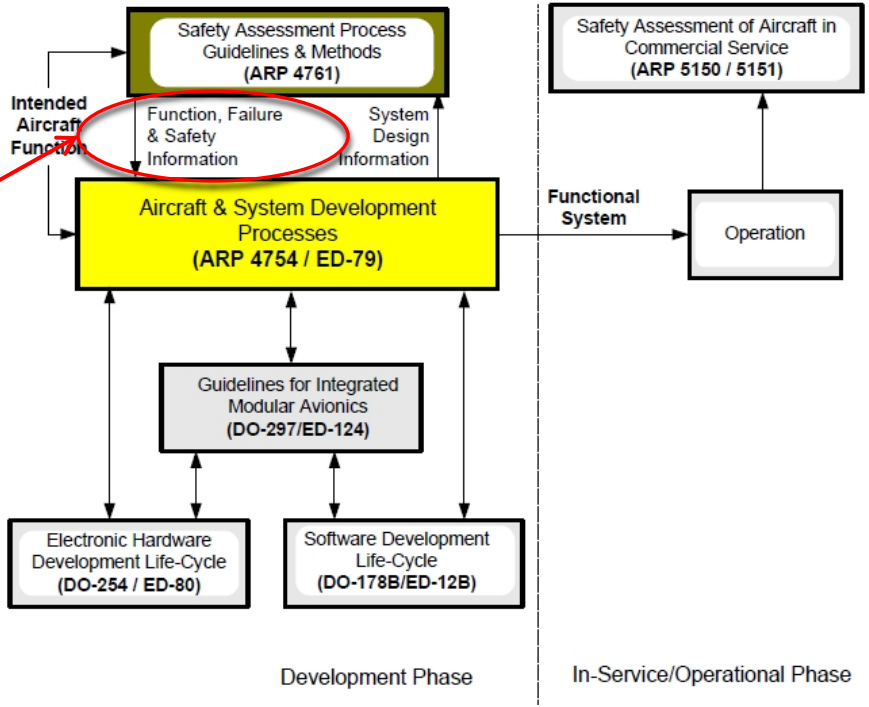
SAFETY SECURITY



Luckily the safety process gives us entry points for security reqs.

Adding security to safety at the functional level

SAFETY SECURITY



We can add failure modes due to security events and monitoring requirements

Security events will generate failure modes

Summary

- Given increased device connectivity, safety-only systems are more vulnerable
- Adding security requirements into safety processes will enable safe incorporation of security features
- Protect against only realistic threats to keep costs down and performance up
- Systems must be designed assuming security functions will require updates at more frequent intervals than safety functions
- Safety engineers and security experts must work together at system level to define requirements which will result in a “Safe and Secure” system

Safety and security can peacefully co-exist

Thank you!

mercury systems™