



Cyber Safety & Security for Reduced Crew Operations

Kevin Driscoll

This work was performed under
NASA contract NNC11BA15B.

Honeywell

Reduced Crew Operations (RCO) would be more than “Flight Management on steroids”

An RCO system will

- have to be ***highly invasive into most, or all, existing safety-critical aircraft systems***
- require a ***highly-reliable data communication*** system that offers very low latency and jitter, as well as high data integrity and authentication

Levels of autonomy and authority (CRM)

- **Cockpit Crew (CC) vs Ground Crew (GC)**

- CC is flying, GC is just standby redundancy
- CC is flying, GC is active second pilot
- GC is flying, CC is active second pilot (PNF)
- GC is flying, CC is just standby

creates

- GC is flying, CC is an adversary or is suicidal?! }
- CC is flying, GC is an adversary (spoofed)?!?! }

**mutually
exclusive**

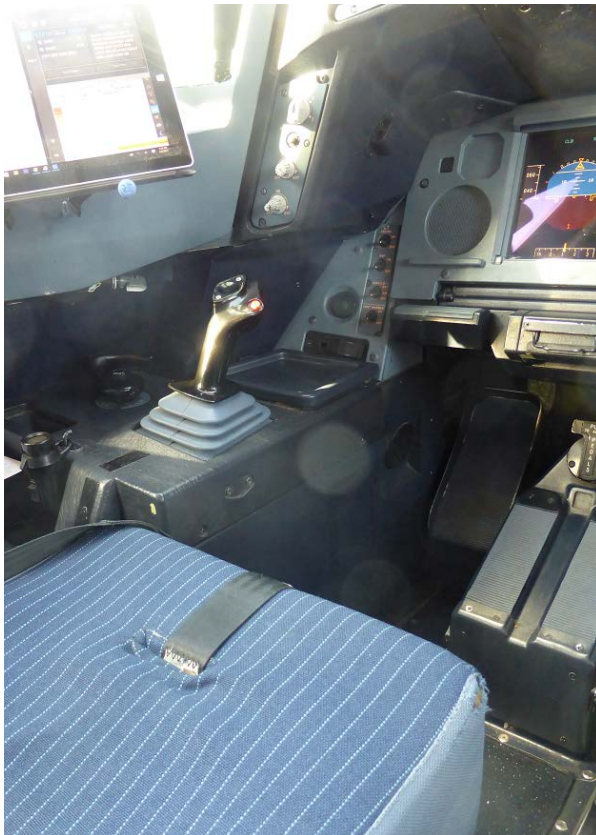
- **Can RCO be used to assist (partially) able-bodied airborne crew?**
- **... totally incapacitated airborne crew?**
 - In the UK, there were 32 in 2009 and 36 in 2004 (~1 per 10 days)
- **Can a GC via RCO be used to override a “rogue” cockpit crew?**

Onboard Safety-Critical Systems

- Traditional 3 layers of aircraft control automation

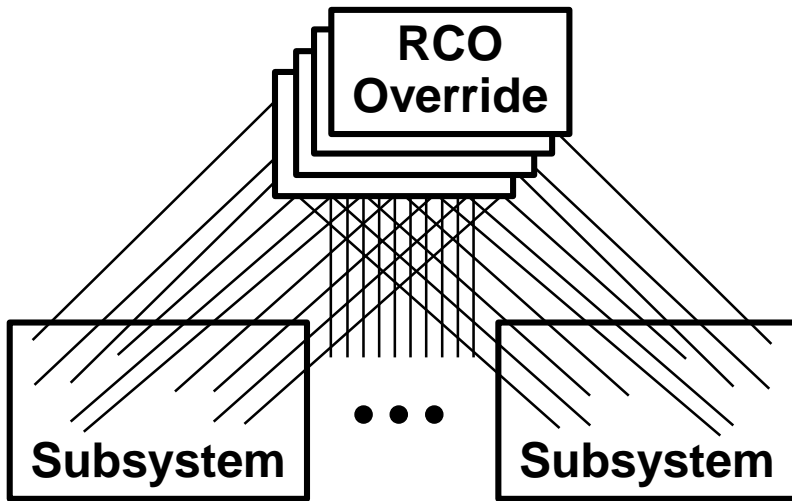
more authority,
but more stringent
latency

- Flight Management System
 - Auto Pilot
 - Flight Control
- controls
- controls

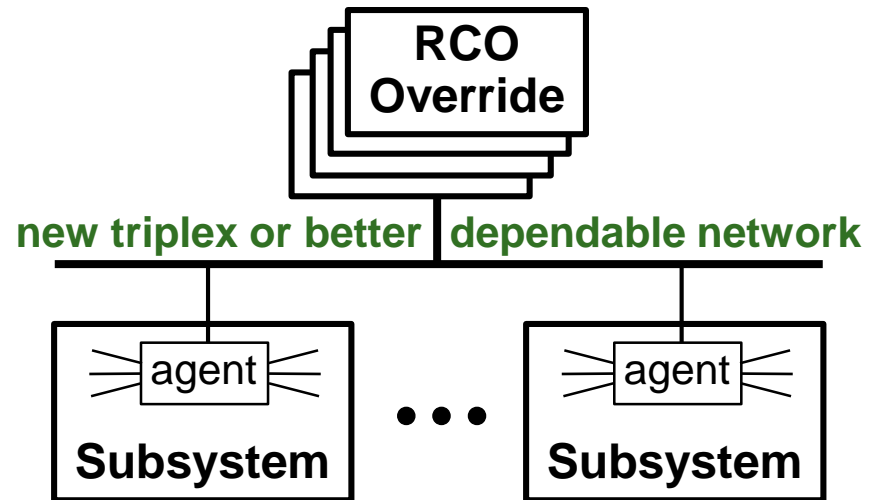


RCO System Architecture

Centralized "Porcupine"

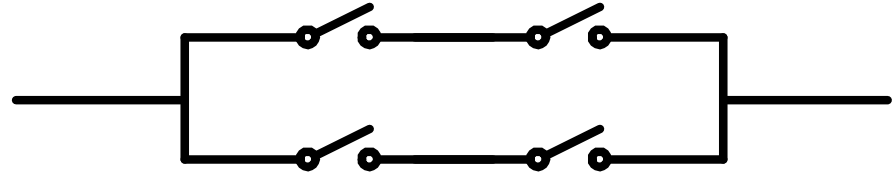


Remote Agents



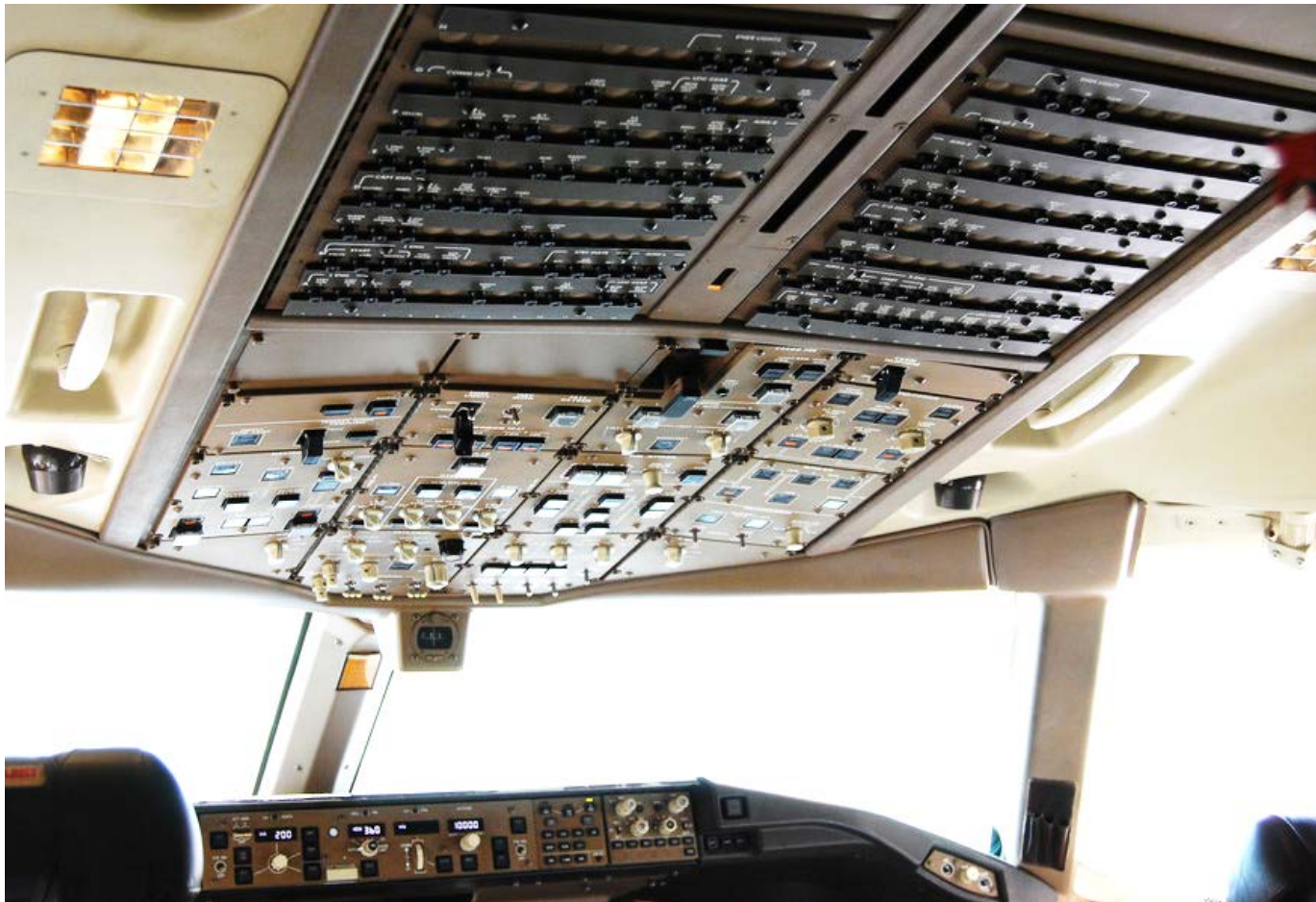
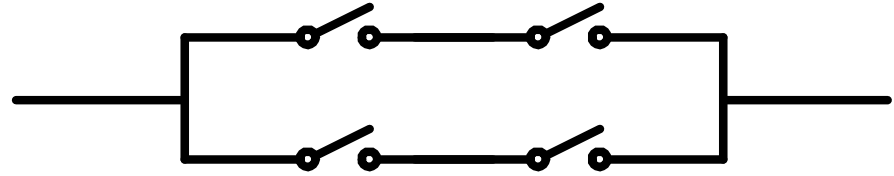
RCO Fault Tolerance

- An RCO system would need to be Byzantine fault tolerant
- Some/most actuators would have to be quad redundant



RCO Fault Tolerance

- An RCO system would need to be Byzantine fault tolerant
- Some/most actuators would have to be quad redundant



Don't Re-invent the Wheel

- Not much R&D done for aircraft RCO safety/security
- Looked at R&D done in adjacent fields
 - UASs (drones)
 - Autonomous ground vehicles (shared control)
 - ◆ “*Right now, there's no good answer*, which is why we're kind of avoiding that space”

-- Dr. Ken Washington
Ford VP

Control Hand-Back Problems

- **Paul Schutte:**
 - “computers [...] give up at the first sign of trouble”
- **Scenarios**
 - **When at the controls, time to regain situational awareness**
 - ◆ Air Canada 878: napping
 - ◆ Audi
 - ◆ Qantas Flight 32
 - **Time to get to the controls, when in cockpit**
 - ◆ Aeroflot 593: kids at the controls
 - **Time to get to the controls, when out of cockpit**
 - ◆ Delta (Chautauqua) 6132: captain stuck in the WC

Typical Abnormality Requiring Crew to Leave Cockpit

Honeywell



Fire trucks surround my
Seattle to Beijing airplane

Are There Real Communication Threats?

- **Individuals**
 - Officially called “phantom controllers”
 - ◆ UK: 18 times in 1999
 - Jim Epik’s book “Phantom Controller” and petition to encrypt ATC
- **Groups**
 - 1981 PATCO
 - Opposing factions in civil wars
- **Nation-State sponsored**
- ***Yes, we have to assume there will be bad actors who are out to get us.***

Some Crypto Key-Management Issues

- **Two aspects of key-management**
 - **Trust**
 - **Logistics**
 - ◆ Key distribution and management
 - *Distribution needs secrecy even if these keys are used only for authentication, not secrecy!*
- **Invention to mitigate logistic issues for avionics**
 - No secrets stored on aircraft
 - Simplifies the airborne side of link
- **Issue: Whose keys?**
- **(Inter)national cryptography laws**

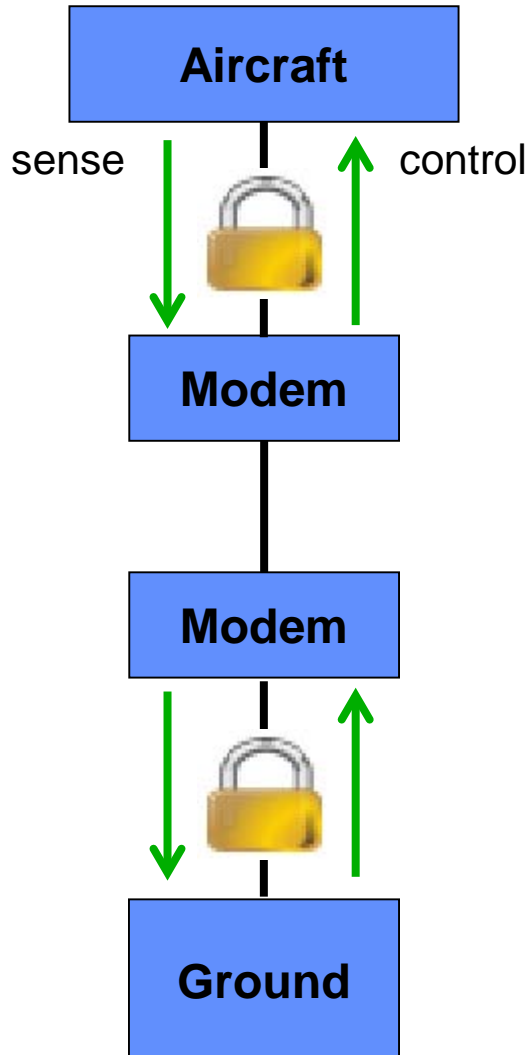
Cryptography Import Laws

Country	Status	Updated
Angola	Unknown ↗	2000
Armenia	Green/Yellow ↗	2000
Bahrain	Yellow ↗	2008
Belarus	Red ↗	2008
Brunei Darussalam	Yellow/Red ↗	2000
Cambodia	Yellow ↗	2008
Canada	Green ↗	2015
Czech Republic	Green/Yellow ↗	2008
China	Yellow ↗	2008
Egypt	Yellow ↗	2007
Ghana	Green ↗	2008
Hong Kong	Green/Yellow ↗	2008
Hungary	Green/Yellow ↗	2008
India	Green/Yellow ↗	2008
Iran	Yellow ↗	2008
Iraq	Red ↗	2000
Israel	Yellow ↗	2008
Khazakstan	Yellow ↗	2008
Latvia	Yellow ↗	2008
Lithuania	Yellow ↗	2008
Malta	Yellow ↗	2000

Country	Status	Updated
Moldova	Yellow ↗	2008
Mongolia	Red ↗	2000
Morocco	Yellow ↗	2008
Myanmar (Buma)	Red ↗	2008
Nepal	Unknown ↗	2000
Nicaragua	Unknown ↗	2000
North Korea	Unknown/Red ↗	2008
Pakistan	Yellow ↗	2008
Poland	Green/Yellow ↗	2008
Russia	Red ↗	2008
Rwanda	Unknown ↗	2008
Saudi Arabia	Green ↗	2008
Singapore	Green ↗	2008
South Africa	Green/Yellow ↗	2008
South Korea	Yellow ↗	2008
Tatarstan	Unknown ↗	2000
Tunisia	Yellow/Red ↗	2008
Turkmenistan	Red ↗	2000
Ukraine	Yellow ↗	2007
Uzbekistan	Red ↗	2000
Vietnam	Yellow ↗	2008

- **Red:**
Total ban
- **Yellow:**
License required for importation
- **Green:**
No restriction
- Taken from:
en.wikipedia.org/wiki/Restrictions_on_the_import_of_cryptography

Latency Problem?



Does the sum of all these added latencies exceed the round-trip latency constraints?

Problems with existing cryptography when applied to cyber-physical systems

- **Slow startup for each key change**
- **Use too much data memory**
- **Need more communication bandwidth**
- **Use separate secrecy and integrity algorithms or added integrity mode**
- **Many new cyber-physical cryptography installations will be retrofits, which further exacerbates the above problems**
- **These are the reasons we created an algorithm (called BeepBeep) specifically for real-time and/or retro-fit applications.**

- **A high-capability RCO system:**
 - May introduce significant safety and security hazards
 - Could be a “single point of failure” for the entire aircraft
- **Technology not ready yet**
 - Research is needed into designing multi-chapter “Level A+” systems
 - Research is needed into the use cryptography for low-latency and international applications
- **RCO capability may be acceptable in the more near term for Part 135, cargo flights, and/or restricted routes and airfields**

**Thank you for your
attention.**

Questions?

Honeywell