Cyber Safety and Security for Pilot Assistance

Kevin Driscoll

This work was performed under
NASA contract NNC11BA15B.

Honeywell

Overview and Problem Statement

Honeywell

- This presentation contains some results from a program Honeywell recently performed for NASA.
- Problem Statement: Significant safety and security hazards can be introduced when avionics systems are enhanced to provide high-authority or even full-authority pilot assistance. This is more than "Flight Management on steroids"; the distinction being that the pilot assistance examined here would have control access to most, if not all, the controls that the crew has access to in the cockpit. This pilot assistance capability could be supplied by some combination of on-board automation and/or ground-based crews and could be used for:
  - Reducing the workload of existing crews
  - Temporarily replacing an incapacitated crew member
  - Replacing the remainder of the crew for single pilot operations
  - Providing a ground crew interface for reduced crew operations

Cockpit Crew (CC) versus Pilot Assistance (PA)

Honeywell

- **There are several scenarios for differing levels of autonomy and authority of PA versus CC as to who is pilot in command (PIC) and other responsibilities (CRM)**
  - **CC is pilot in command, PA is just standby redundancy**
  - **CC is pilot in command, PA is active second pilot**
    - "Another pair of eyes" (sharing the "see and avoid" responsibility)
    - What are the PA's "eyes"? — add multiple video cameras, transponders?
  - **PA is pilot flying, CC is active second pilot (PNF)**
    - Recovery time issue (if ground communications or onboard systems fail)
  - **PA is pilot in command, CC is just standby**
    - More recovery time (if ground communications or onboard systems fail)
    - Various degrees of the AC being "out of the loop"
      - In cockpit: eating, doing logbook, working on schedule, napping, etc
      - Out of cockpit: lavatory, sleeping, checking on abnormalities, etc

creates

  - **PA is pilot in command, CC is an adversary or is suicidal?!**
  - **CC is pilot in command, PA is an adversary (spoofed)?!?!**
    - Such a design would violate "do thy patient no harm" principle (***new cyber attack pathway into the aircraft***)

mutually exclusive

Pilot Assistance Authority

Honeywell

- **Some questions:**
  - **Can the pilot assistance override the cockpit crew? Under what use cases and *who acts as the arbitrator*?**
  - **To what extent should we address rogue pilots? How many of the ways a rogue pilot can crash an airplane can/should we protect against (e.g., lowering the landing gear at speed, differential flaps, all of the critical circuit breakers on the cockpit ceiling)?**
  - **Where does pilot assistance interface into aircraft systems?**
  - **What protections do we provide for normal aircraft system component failure versus malicious human influence?**
    - "Murphy versus Satan" (natural failures vs human threats, respectively) ***For 10e-9 requirements, Murphy is indistinguishable from Satan, except for coordinated attacks against independent components***
  - **What is the proper balance of integrity versus availability?**
    - ***Simple dual redundancy can give you availability or integrity, but not both!***

Onboard Safety-Critical Systems

Honeywell

- **Traditional three layers of aircraft control automation**

more authority, but more stringent latency

  - Flight Management System (planning, source-to-destination profile)
  - Auto Pilot (altitude, heading, speed)
  - Flight Control (stick and rudder – attitude control, stability)

controls

controls

Expected dependability requirement for pilot assistance is 1e-9, which is the same as for Flight Control and Engine Control

- **Other potentially safety-critical systems**
  - Power
    - Conversion (AC/DC, DC/AC) and distribution (tie relays and switches)
    - Circuit breakers (there are a lot of them)
  - Fuel distribution (center of gravity control, jettison)
  - Flight-control surface trim
  - Landing gear
  - Spoiler, thrust reverse, and braking systems
  - De-icing and pitot heat
  - Radio tuning?
  - . . .

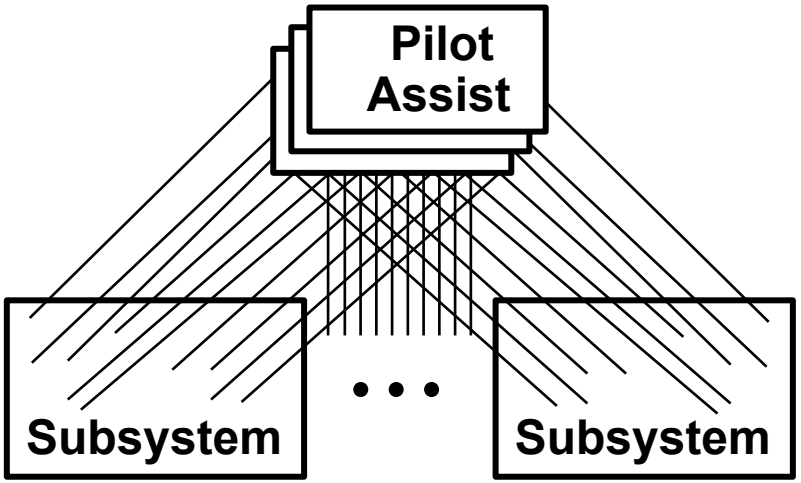
- **This degree of invasiveness likely not foreseen by proponents of pilot assistance who maybe only thinking about intercepting only the control path from stick/rudder to flight surfaces**

Pilot Assistance System Architecture

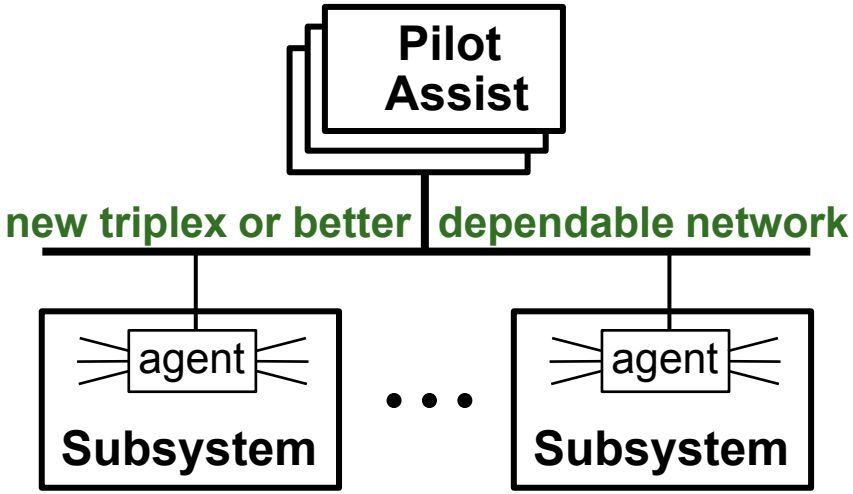
Honeywell

- Depending on requirements for handling rogue pilots, may need to intercept ***all*** systems that could possibly cause an aircraft to not continue safe flight (including systems not in the three traditional control layers: FMS, autopilot, flight control).
- Even without a rogue pilot (i.e., just "benign" incapacitation) many systems will need to be intercepted to provide pilot assistance override (dying pilot falls on stick or flails and hits <…>).
- A couple of possible on-aircraft architectures (both are expensive, safety-critical, and highly disruptive to current aircraft systems):

Centralized "Porcupine"



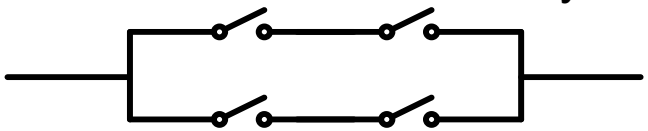
Remote Agents



Pilot Assistance Fault Tolerance

Honeywell

- **Some actuators would have to be quad redundant**
  - **Example, there is no safe state for circuit breakers**
    - Must be off/open for a short-circuit that could cause a fire
      - That is why they are there
    - Must be on for critical functions
      - Could be M-out-of-N for redundant loads, but which one(s) should be on?
    - There are a lot of circuit breakers
    - Here is the minimum circuit for a fail-op circuit-breaker configuration tolerating one stuck-open or one stuck-closed breaker; this is also needed for some sets of switches and relays that need to be fail-op



- **For a pilot assistance computer system to tolerate just one Byzantine Failure (a fault that shows different symptoms to different observers and causing those observers to disagree), it has been well established (mathematical proof, thousands of refereed papers) that a minimum of four fault zones and three independent communication paths are required.**

Q's and Preliminary A's for Degree of Authority

Honeywell

Q: Can pilot assistance be used to assist a (partially*) able-bodied cockpit crew?

A: Yes, This is the most studied and easiest case.
Cost would depend on the degree of assistance.

Q: Can pilot assistance be used to take over for totally incapacitated* cockpit crew?

A: This probably would be required for SPO, RCO, hypoxia events.

Too invasive and expensive to retrofit into existing aircraft.
Possible, but still very invasive and expensive for future aircraft designs.

May have the same security issues as the next question (next slide). That is, if the crew is *not* incapacitated, can they prevent bad pilot assistance control (Murphy or Satan) from taking control, given this level of invasiveness?

*** Note: It is not uncommon to have an incapacitated crew member.**
In the UK, there were 32 in 2009 and 36 in 2004 (~1 per 10 days).
This actually is better than the 1% probability per year rule.

Q's and Preliminary A's for Degree of Authority (cont)

Honeywell

Q: Can pilot assistance be used to override a compromised cockpit crew (e.g., suicide, active incapacitation)?

A: This leads to some troubling questions. Who has the *ultimate* authority? The answer to this must be the same for all situations. Otherwise, who has the authority to decide what the situation is? Obviously, the ultimate authority would have to be the pilot assistance for this level of control. But, why should pilot assistance be any less prone to being bad (Murphy or Satan) than an cockpit crew? One can argue that there is a greater probability for ground-based pilot assistance going rogue (they don't have to face certain death) and they can crash more than one aircraft. One could envision a redundant ground crew. But, they would have to be totally independent (including independent communication channels to the aircraft) and these redundancies could only be used for integrity, not availability. So, this would require two ground crews to replace one cockpit crew (could be timeshared among a few aircraft). Add this cost of two ground crews to the high cost of very invasive avionics the economics doesn't look very promising.

Don't Re-invent the Wheel

Honeywell

- **Not much research done on safety and security for this degree of pilot assistance authority**
  - **Mostly human factors related (e.g., workload/stress reduction)**
  - **Safety, security, and certification not as well addressed (skipping the difficult stuff = "design procrastination")**
- **Looked at R&D done in adjacent fields**
  - **UASs (no airborne crew to share control responsibility)**
    - Looked at communication issues (availability, safety, and security)
  - **Autonomous ground vehicles (shared responsibility issue)**
    - Looked at issue of full autonomy versus shared responsibility
    - Ford says that the possible interim step to fully autonomous vehicles, where the driving responsibility is shared between an autonomous digital driving system and human drivers, can't be done safely. ***The problem is the handoff from the digital system back to the human driver when something unexpected happens***. Designers can't anticipate every possible situation a vehicle can encounter.
    - "***Right now, there's no good answer***, which is why we're kind of avoiding that space"

-- Dr. Ken Washington
Ford's VP of research and advanced engineering

Source of Control Hand-Back Problems

Honeywell

- **Paul Schutte, in his "How to Make the Most of Your Human" presentation for HCI International 2015, had a slide which said:**
  - One reason why computers are so reliable at what they are programmed to do is because they *give up* at the first sign of trouble.
  - When the autopilot reaches its maximum authority, it throws up its hands and tosses control back to the human, whether the human is ready for it or not.
  - Pilots routinely must intervene whether it's simply resetting a circuit breaker or turning off the automation.
  - The main reason why humans are still on the flight deck is to manage risk by dealing with or avoiding the unexpected, unanticipated, or complex situations

Control Hand-Back Problem Scenarios

Honeywell

- The time it takes for a crew to regain control after a hand-back depends on what the crew was doing at the point the pilot assistance throws the control back to the crew, examples various levels follow
- Time to get to the controls, when out of cockpit
  - Delta (Chautauqua) 6132: captain stuck in the lavatory due to door latch being broken, had to breakdown the door
  - A common reason for leaving the cockpit is to investigate an abnormal situation (e.g., smoke). One can argue this is precisely the wrong time to leave the cockpit unattended. The abnormality being investigated could cause a loss of RCO communication or the on-board pilot assistance or its interfaces to critical systems.
    - First corollary of Murphy's Law: When things do go wrong, they will go wrong at the most inopportune time.

Typical Abnormality Requiring Crew to Leave Cockpit

Honeywell

A half-hour into a scheduled 12-hour flight, a cockpit crew member rushed to the rear of the airplane to investigate the smell of smoke. For RCO or SPO, this would have been the whole crew (!), away from the cockpit for a significant amount of time. This is not a very unusual scenario. The airplane returned to Seattle for over-night repairs.

Control Hand-Back Problem Scenarios (cont.)

Honeywell

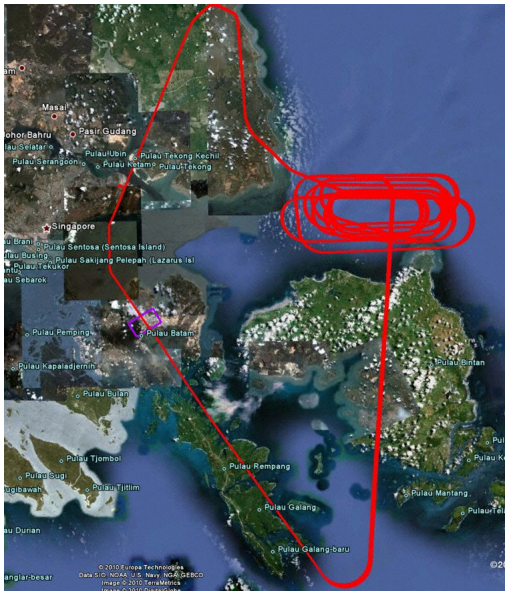
- Time to get to the controls, when in cockpit
  - Aeroflot 593 (A-310): Pilot's son accidently disengaged the autopilot. Children in the way plus g-forces prevented crew getting back into their seats and at the controls in time. All 63 passengers and 12 crew members died in crash.
- Once at the controls, time to regain situational awareness under normal conditions
  - Air Canada 878 (B-767): "Under the effects of significant sleep inertia (when performance and situational awareness are degraded immediately after waking up)" a pilot mistook the planet Venus as lights of another airplane on a collision course and dove to avoid it. When the plane nosedived, 14 passengers and two crew members were injured because they were not wearing seatbelts.
  - Audi says its tests show it takes an average of 3 to 7 seconds, and as long as 10, for a driver to snap to attention and take control, even with flashing lights and verbal warnings.

Control Hand-Back Problem Scenarios (cont.)

Honeywell

- "… anyone who gets behind the wheel [of an semi-autonomous car] must be properly trained. For Audi, this means learning to be a *better than average driver*. […] *if you need to grab the wheel, the odds are something's gone terribly amiss*." *

- **Recovery time can be even longer if diagnosis is required**
  - Qantas Flight 32 A380 engine disintegration: Needed 50 minutes and 5 crew to sort out all the ECAM messages (crew had no time for ACARS) before landing (lucky to have 3 normal crew plus Check Captain and Supervising Check Captain)



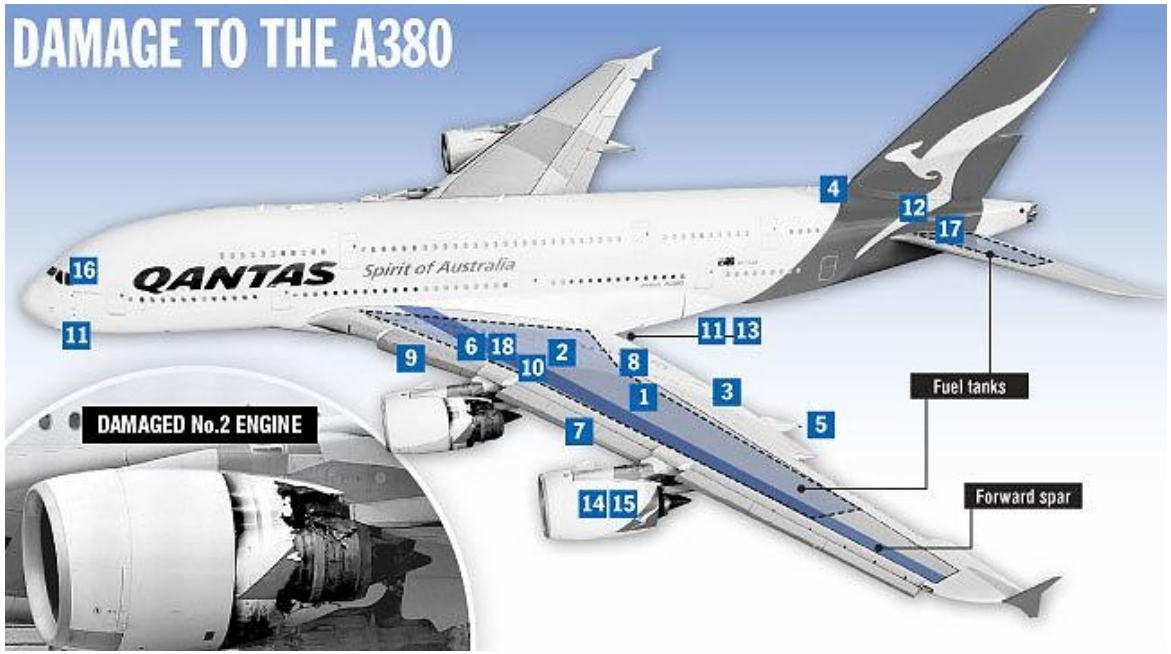
- **Dealing with abnormal situations may require *additional* airborne crew, versus a reduction in crew**

* www.wired.com/2015/01/rode-500-miles-self-driving-car-saw-future-boring
emphasis added

Qantas A380 Engine Fan Blade Separation

Honeywell

1 Massive fuel leak in left mid fuel tank -- there are 11 tanks, including tail's horizontal stabilizer
2 Massive fuel leak in the left inner fuel tank
3 A hole on the flap fairing big enough to climb through
4 Aft fuel system failed, preventing many fuel transfer functions
5 Problem jettisoning fuel [180K lbs]
6 Massive hole in the top of wing
7 ~~Partial~~ failure of leading edge slats
8 Partial failure of speed brakes and ground spoilers [and ailerons]
9 Shrapnel damage to the flaps
10 Loss of all hydraulic fluid in one of the jet's two systems
11 Manual extension required for landing gear [gravity drop]



12 Loss of one generator and associated systems [electrical busses 1 and 2 failed]
13 Loss of brake anti-skid system
14 No.1 engine could not be shut down in the usual way after landing because of major damage to systems
15 No.1 engine could not be shut down using the fire switch, which meant fire extinguishers wouldn't work
16 There were 58 different ECAM warning messages, plus an unknown number of ACARS messages
17 Fuel was trapped in the trim tank (in the tail) creating a balance problem for landing
18 Left wing forward spar penetrated by debris

Only one engine (of 4) was working normally with thrust reversing. Four blown tires. Leaked fuel on 1600°F wheels.

Richard Woodward (a Qantas A380 pilot and deputy president of the Australian and International Pilots Association) said that the "number of failures is unprecedented, […] There is probably a one in 100 million chance to have all that go wrong." But, there have been over a half-dozen previous similar incidents (Sioux City DC-10 crash is well known).

"Those who cannot remember the past are condemned to repeat it."

Are There Real Communication Threats?

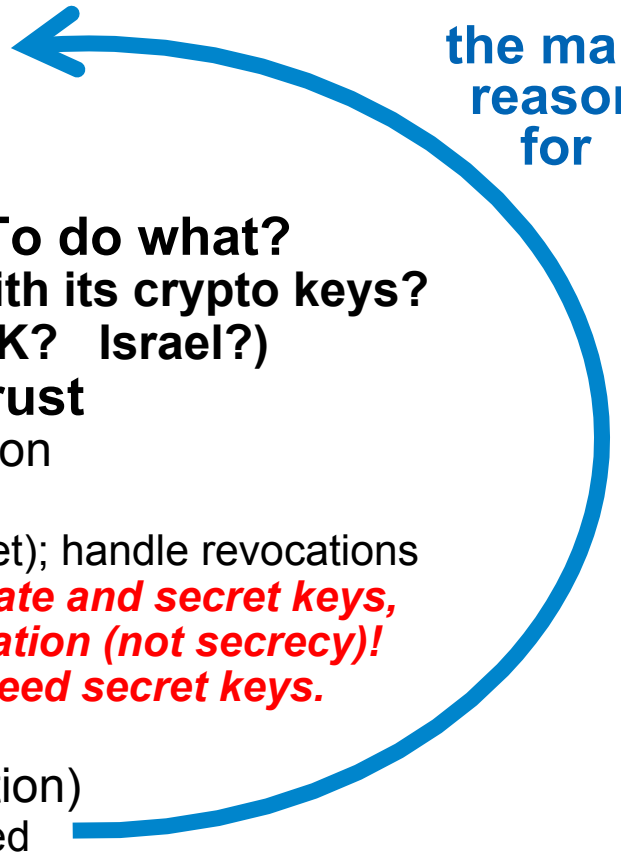
Honeywell

- **Would someone really try to interfere with the flight of an aircraft equiped with pilot assistance or is this just a "Hollywood" fantasy?**
- **"Just because you're paranoid, that doesn't mean that they are not out to get you."**
  - **Individuals**
    - Officially called "phantom controller" (a.k.a., "bogus", "fake", "phony")
      - U.K. (18 in 1999), U.S. ("several times a year")
    - Underreported (this is hard to verify, but from reasonable sources)
    - Jim Epik's book "Phantom Controller" and petition to encrypt ATC comm's
  - **Ad hoc / transitory groups**
    - 1981 PATCO, some striking members became phantom controllers
    - Opposing factions in civil wars
  - **Nation-State sponsored**
    - Air France flying back from Japan (indications it was North Korea)
    - Air France told to dump fuel on Tokyo (North Korea again or individual?)
- ***Yes, we have to assume there will be bad actors who are out to get us.***

Some Crypto Key-Management Issues

Honeywell

- **(Inter)national cryptography laws**
  - **Export, import, usage, key management**
- **Two aspects of key-management**
  - **Trust: Who do you trust? With what? To do what?**
    Example: Can an airline trust the US? … with its crypto keys?
    (reveal keys to: North Korea? UK? Israel?)
  - **Logistics: Mechanisms to enforce the trust**
    - Creation of keys and their ownership/association
    - Key distribution and management
      - Only allows authorized users for a set time (sunset); handle revocations
      - ***Distribution needs secrecy protection for private and secret keys, even if these keys are only used for authentication (not secrecy)! Popular authentication schemes (e.g., MAC) need secret keys.***
    - Ordinary use (e.g., RCO communications)
    - Extraordinary use (e.g., government investigation)
      - Need access to "plaintext" that has been encrypted
        » "Easiest" and most common method is to give government access to the keys
        (But, still can greatly complicate key distribution and management)
    - Just "use X.509 based public key infrastructure (PKI)" ??
      But: Full PKI is heavy weight and doesn't solve all the problems by itself



- **Invention to mitigate most of these issues for avionics**
  - **No secrets stored on aircraft, simplifies the airborne side of link**

Cryptography Import Laws

Honeywell

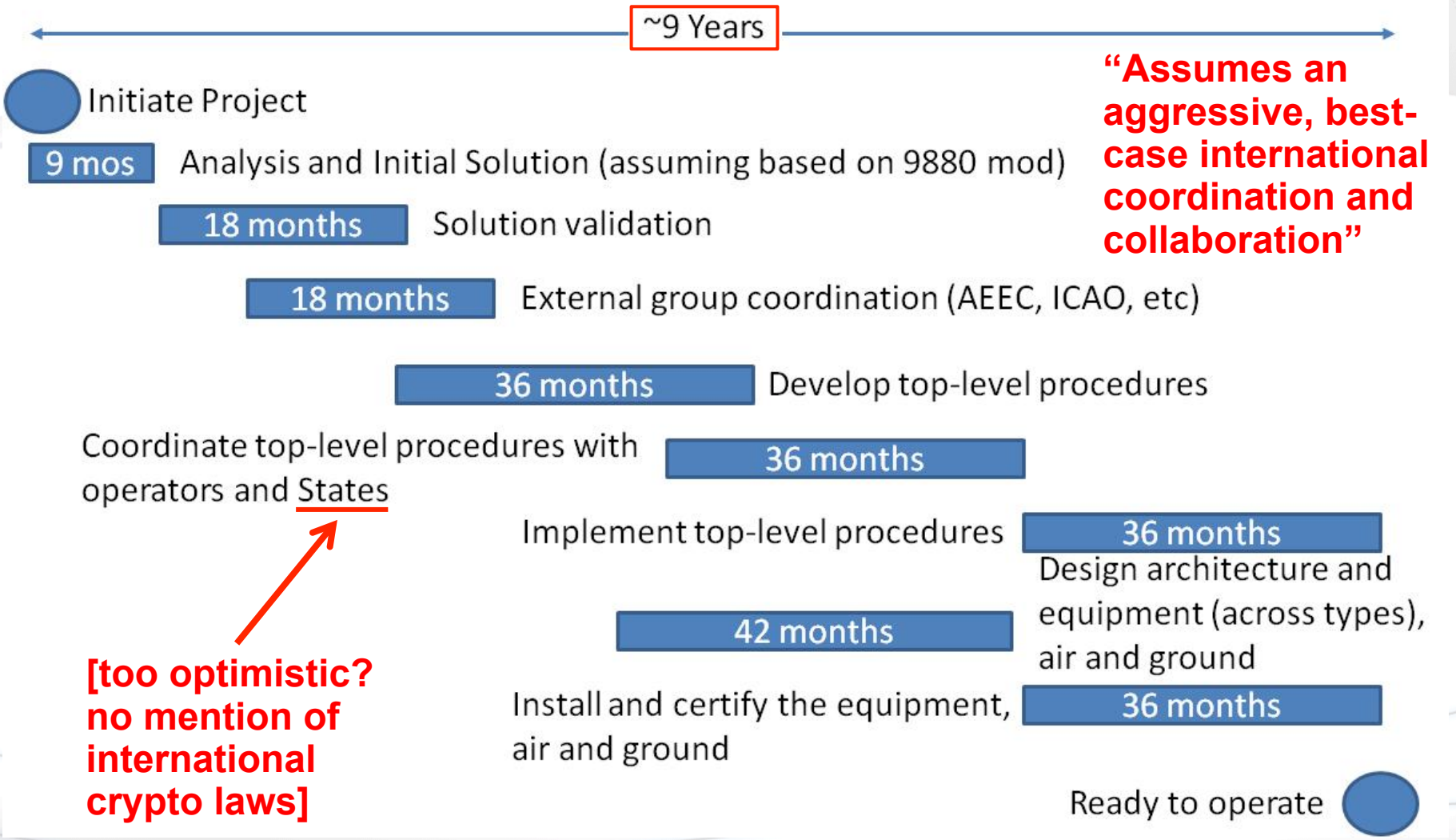
Country	Status	Updated
Angola	Unknown	2000
Armenia	Green/Yellow	2000
Bahrain	Yellow	2008
Belarus	Red	2008
Brunei Darussalam	Yellow/Red	2000
Cambodia	Yellow	2008
Canada	Green	2015
Czech Republic	Green/Yellow	2008
China	Yellow	2008
Egypt	Yellow	2007
Ghana	Green	2008
Hong Kong	Green/Yellow	2008
Hungary	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 (Burma)	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

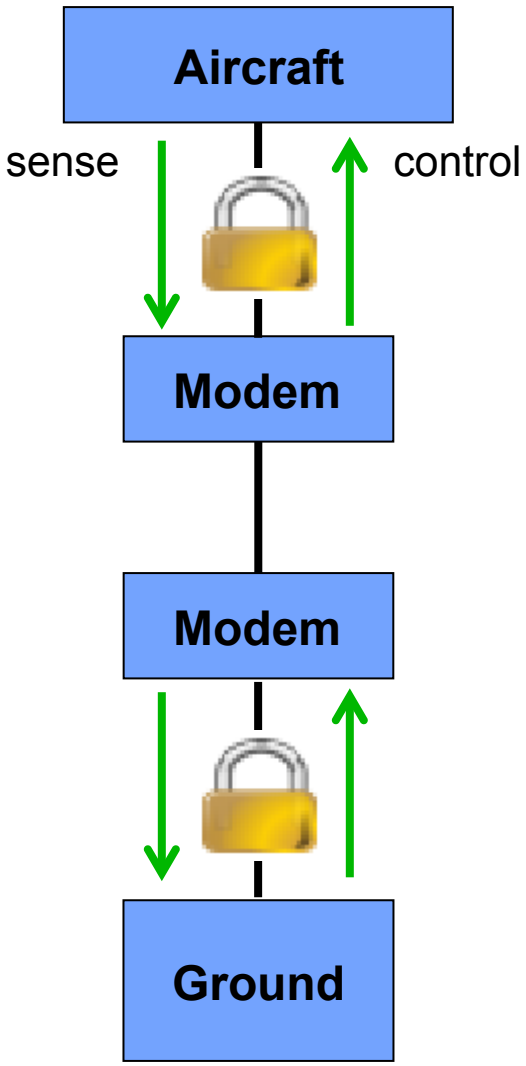
- Taken from: en.wikipedia.org/wiki/Restrictions_on_the_import_of_cryptography

Security Roadmap



Latency Problem?

Honeywell



Each transmission loop incurs the **latency of two encrypts and two decrypts**. If AES (or similar block cipher) is used to provide secrecy and integrity, a block (e.g., 128 bits) of store-and-forward latency has to be added, plus the latency for any added initialization vector (IV) and/or integrity data (e.g., 32 bits each). These latencies depend on communication speed (the slower the link, the longer these latencies) and they have to be added to the crypto computation latencies. The sum of these latencies doubles if handshakes (e.g. ACK/NAK) are used and are encrypted.

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

UASs solve this problem with very high-speed (e.g., 10 Gbps) communication links and special hardware encryption (e.g., KG-340 encryptors and Single-Chip Crypto field programmable gate arrays) or use video compression (which is still > 10 Mbps per video stream).

Problems with existing cryptography when applied to cyber-physical systems

Honeywell

- Slow startup for each key change (due to “key scheduling” being done)
  - Small messages and sessions, less data over which to amortize startup cost
  - Latency (delay) and jitter are usually more important than throughput
  - Only worst case timing counts, average is unimportant
    - A missed real-time deadline not helped by finishing early at all other times
- Use too much data memory
  - Cyber-physical software is multitasking with many context switches / sec that cause a task’s cache entries to be evicted (replaced with other tasks’ data and instructions)
  - To guarantee timing, one must assume most memory accesses cause cache misses
  - But, existing crypto performance info (propaganda) assume a “pre-warmed” cache
  - Even L1 cache ***hits*** can be expensive (equivalent to a half-dozen instructions)
- Need more communication bandwidth than may be available
  - Bandwidth for: key management, initialization vectors, integrity check data, pads, …
- Use separate secrecy and integrity algorithms or added integrity mode
  - Makes execution even slower and uses more power
  - The added latency can preclude “lump in the cable” retrofits
- 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.

Conclusions

Honeywell

- A high-capability pilot assistance system:
  - may introduce safety and security hazards depending on how much authority the crew relinquishes to the pilot assistance
  - could be a “single point of failure” for the aircraft due to its authority over all (or almost all) safety-critical cockpit controls
    - Similar problems could be faced by future highly-integrated cockpits
- More research is needed into the design of multi-chapter “Level A+” systems that could be an aircraft’s single point of failure
- More research is needed for using cryptography to cover the real communication threats to ground-based pilot assistance
  - Is special-purpose low-latency encryption needed?
  - What must be done to allow legal use of encryption in all the different jurisdictions an aircraft may encounter?
- Such a capability may be acceptable in a more near term for Part 135, cargo flights, and/or restricted routes and airfields

Thank you for your attention.

Questions?

Honeywell