Air Traffic Control

source: FAA
Electronic Flight Bags

source: AeroPlan Systems
Field Loadable Software

source: fordforums.com.au
Commercial aviation Safety Record

World 2009-2013

- Runway / Taxiway Excursion
- Gear-up Landing / Gear Collapse
- Ground Damage
- Hard Landing
- In-flight Damage
- Tailstrike
- Undershoot
- Other End State
- Off Airport Landing / Ditching
- Mid-air Collision

Percent of Passenger and Crew Fatalities Relative to Total Onboard

Note: Circle size increases as total fatalities increase; circles with white centers indicate no fatalities.

source: IATA
So why look at security now?

Things are changing

- Need to increase NAS capacity → NextGen and ADS-B
- Systems are increasingly being connected (Gatelink, internet)
- Systems are running on shared hardware
- Systems are becoming more standardized
- New adversaries and adversary capabilities
Field Loadable Software

From the Boeing website:

“Modifying system functionality with new software instead of with modified or new hardware can help operators reduce the total number of hardware line replaceable units (LRU) in inventory, increase hardware commonality, and reduce airplane modification time.”

Examples:

- Airplane information management system (AIMS)
- Cargo smoke detector system (CSDS)
- Electronic engine control (EEC)
- Flap/slat electronics unit (FSEU)
- Traffic collision avoidance system (TCAS)
- Etc.
Conventional security approach

Manufacturer

Server

Mechanic

upload

download

install
Applying STPA-Sec to Field Loadable Software

FLS is a system that delivers safe software to aircraft components by means of a manufacturer's network of approved repair stations in order to support safe and efficient operations of general aviation.
STPA Losses and Hazards

**Losses:**
- L1: injury or loss of life
- L2: damage to equipment

**Hazards:**
- H1: Aircraft is operated when hazardous FLS is installed → L1, L2
- H2: Aircraft component is powered up when hazardous FLS is installed → L2

**Safety constraints:**
- C1: Aircraft must not be operated when hazardous FLS is installed
- C2: Aircraft component must not be powered up when hazardous FLS is installed
<table>
<thead>
<tr>
<th>Control Action</th>
<th>Context</th>
<th>P</th>
<th>NP</th>
<th>S</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>install software</td>
<td>Software is hazardous</td>
<td>T</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software is not hazardous</td>
<td></td>
<td>T</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>install update</td>
<td>Software is hazardous</td>
<td>T</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software is not hazardous</td>
<td></td>
<td>T</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>check system</td>
<td>Installed FLS is hazardous</td>
<td></td>
<td>T</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Installed FLS is not hazardous</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Control actions (Manufacturer)

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Context</th>
<th>P</th>
<th>NP</th>
<th>S</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make software available</td>
<td>Software is hazardous</td>
<td>T</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Make update available</td>
<td>Update is hazardous</td>
<td>T</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Update is not hazardous</td>
<td>T</td>
<td>T</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issue service bulletin</td>
<td>Current FLS is hazardous</td>
<td>T</td>
<td>T</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Some questions to consider

- How does the mechanic verify if he installed the right software?
- Does it matter if the pilot cannot check the software version himself?
- Does the manufacturer need a formal channel to the pilots?
- Are there reasons for a mechanic not to notify the manufacturer of issues?
- Do we even need a mechanic to update field loadable software?
- What happens if we leave out the mechanic?
Research sponsored by
Federal Aviation Administration

Special thanks to:
Dr. Nancy Leveson
Col. William Young
Dr. John Thomas

Speaker info
Jonas Helfer
PhD candidate in EECS
helfer@mit.edu