PKI: AN AVIATION CASE STUDY

Taking lessons from e-Enabled aircraft management and applying them to critical infrastructure

Ron Brash (Btech, MsCompSci)
Director of Cyber Security Insights
Verve Industrial Protection

VERVE

Disclaimer:

These opinions are my own, and observations I have made do not represent those of my employer, partners, nor past/present/future clients & engagements.

Please be responsible with the knowledge contained here-in

“Lots of people working in cryptography have no deep concern with real application issues. They are trying to discover things clever enough to write papers about.”

WHITFIELD DIFFIE

The Scenario of PKI and e-Enabled Aircraft

- **Consider the complexity** of aircraft and supporting infrastructure

- **Relatively homogenous environment** except:
  - Every single “tail” is different

- **Numerous software parts** to be signed, loaded and managed on a plane, but:
  - **There is a certificate mismatch?**
  - **A part cannibalized from another tail?**
  - **OR an SOP is missed?**
  - **Maintenance is scheduled?**

The Aviation Ecosystem (it's huge)

VERVE

ONBOARD AIRCRAFT SYSTEMS
Avionics, communications, controls,
ONS, EFB, CMS etc.

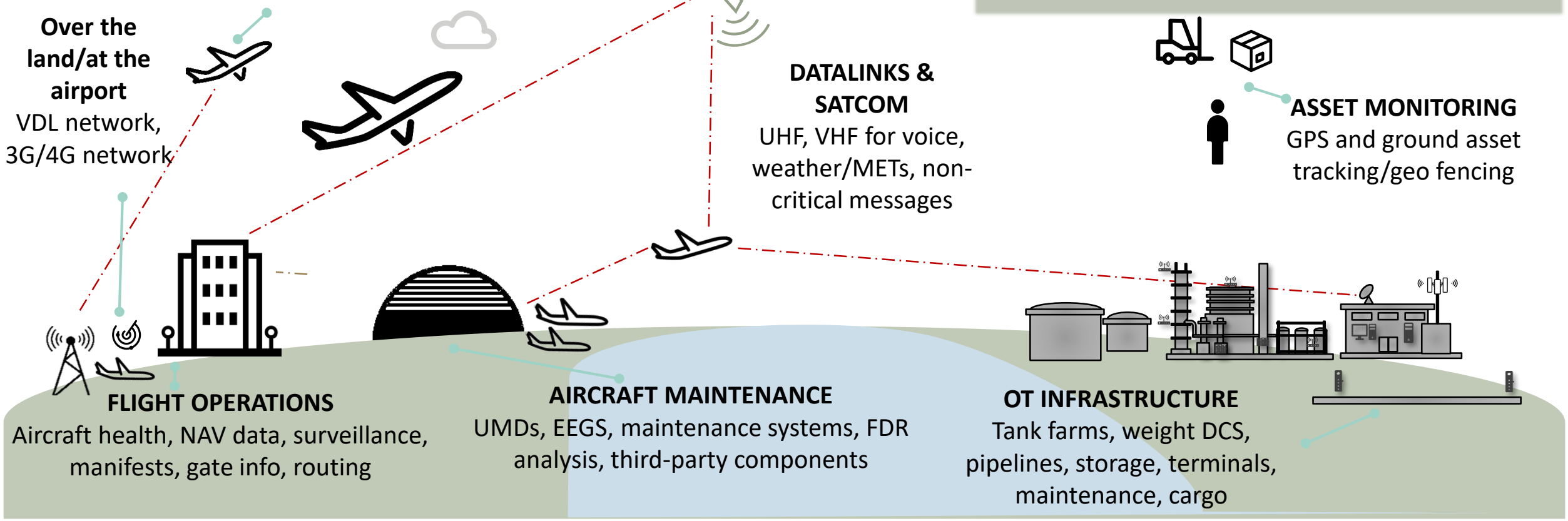
SATCOM
ACARS, ADSB, GPS, IFEC (multimedia, in flight connectivity, BYOD), weather

AIRPORTS
Gate systems, Kiosks, LTE, ATM components, Ops, Gatelink

Over the land/at the airport
VDL network, 3G/4G network

DATALINKS & SATCOM
UHF, VHF for voice, weather/METs, non-critical messages

ASSET MONITORING
GPS and ground asset tracking/geo fencing



FLIGHT OPERATIONS
Aircraft health, NAV data, surveillance, manifests, gate info, routing

AIRCRAFT MAINTENANCE
UMDs, EEGS, maintenance systems, FDR analysis, third-party components

OT INFRASTRUCTURE
Tank farms, weight DCS, pipelines, storage, terminals, maintenance, cargo

Loadable Software Aircraft Parts & Aviation 101

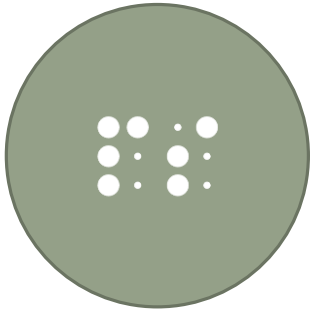
VERVE

What is in it? Where is it used?

Typically, **a Loadable Software Aircraft Part (LSAP)** is:

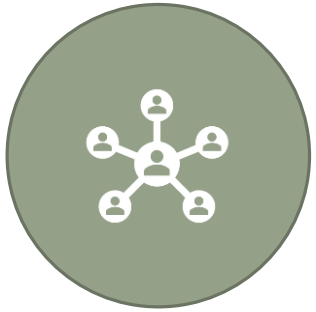
- Anything software or configuration related to be loaded aboard an aircraft.
- **This is also true for non-e-Enabled aircraft** (e.g., standard loadable parts)

CONFIGURABLE ITEMS & FIRMWARE TRACKING



SUPPLYCHAIN & VENDOR AUTHENTICITY

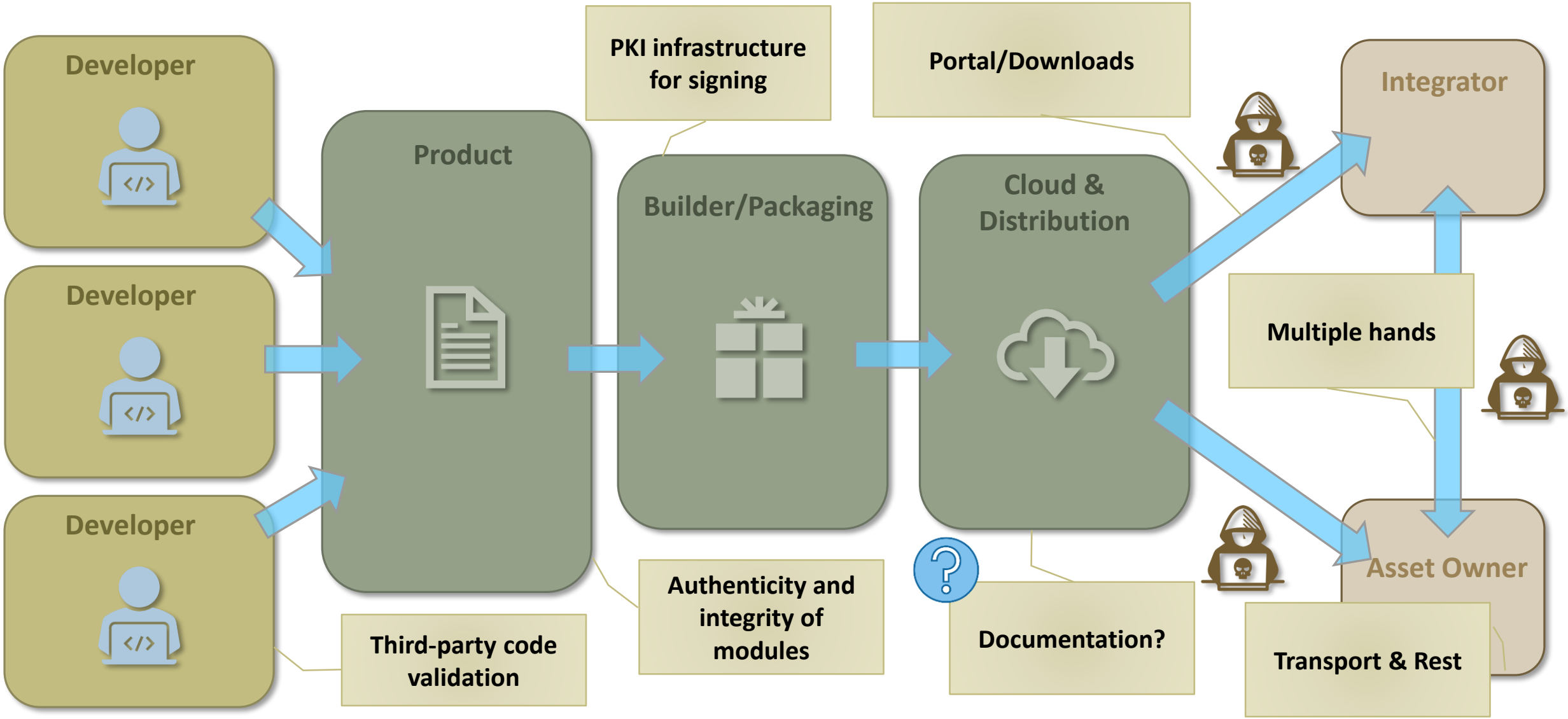
CENTRALIZED PART & SYNCRONIZED FLEET MANAGEMENT



AIRCRAFT INTEGRITY & COMPLIANCE

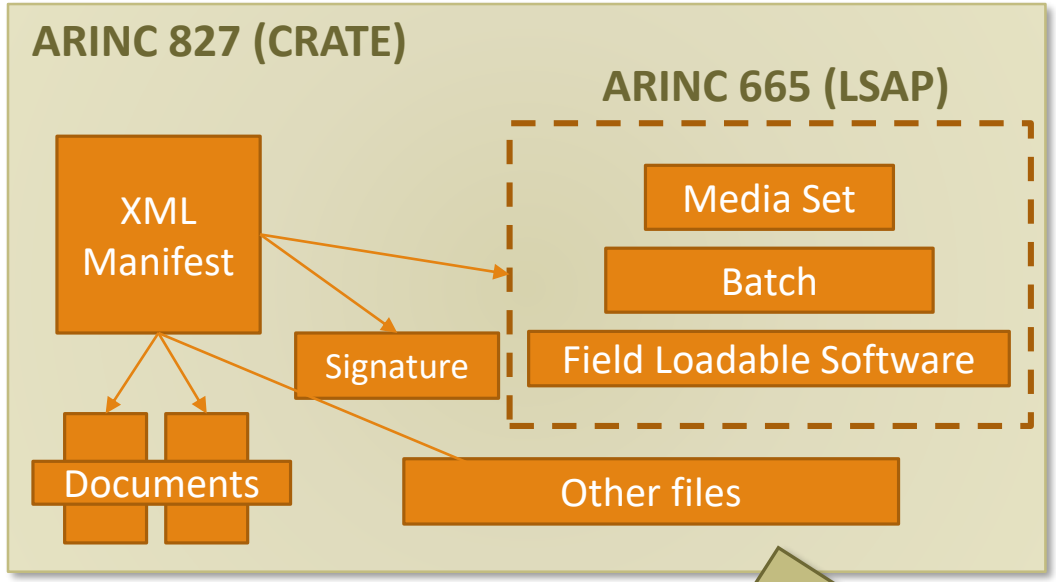
The Case for Signed Firmware – The "short" Why!

VERVE

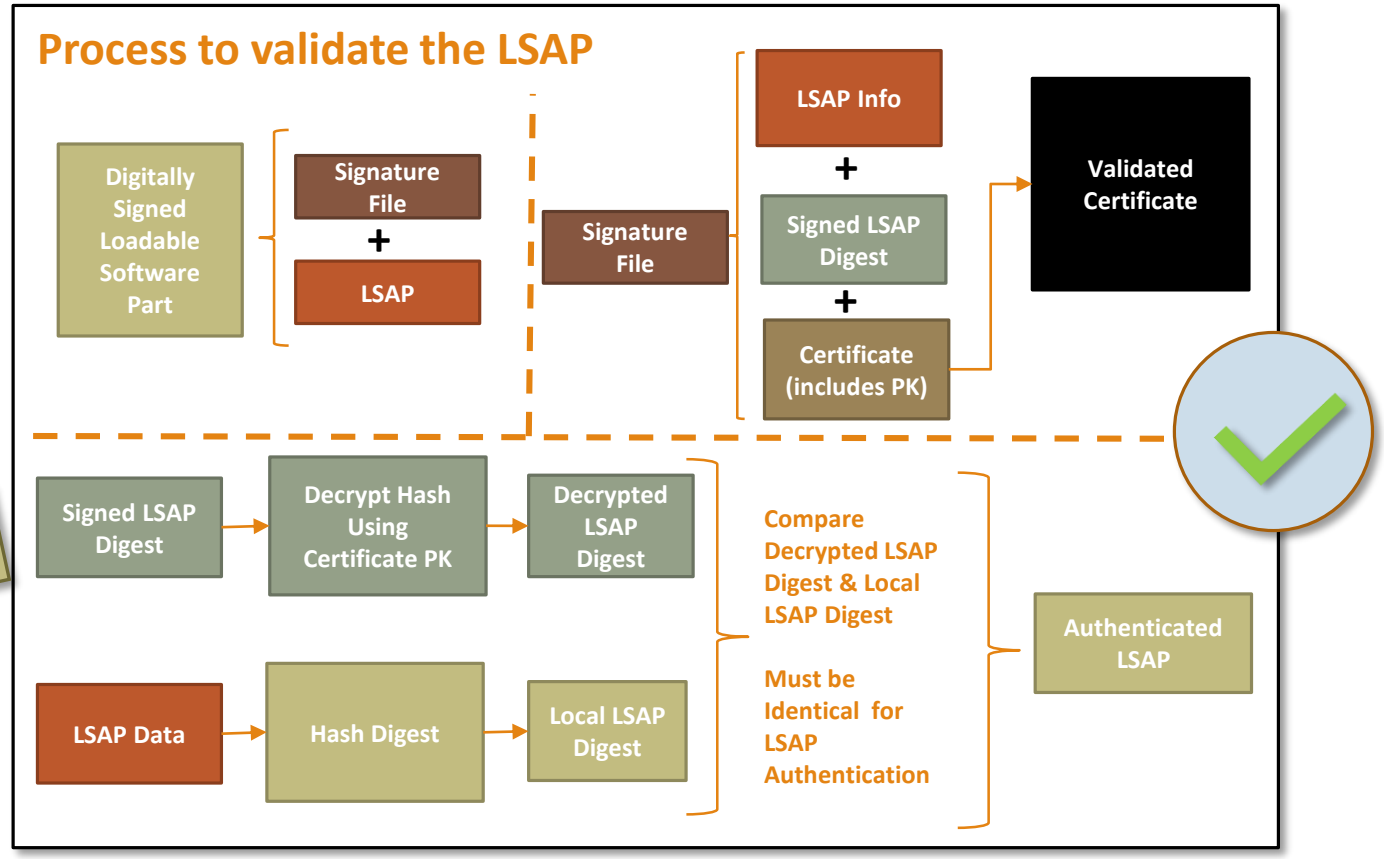


Signed Aviation Firmware generally looks like this (+-)

VERVE



The concept of a CRATE makes sense to me as a traditional engineer (good analogy IMHO)



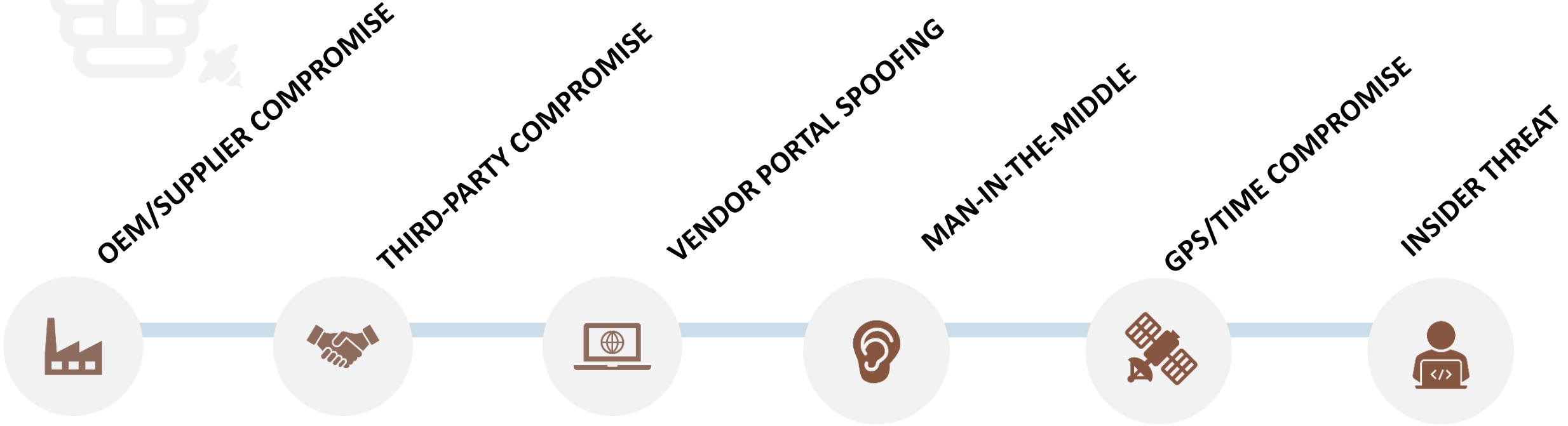
General problems seen with PKI & signed firmware?

- Overall effort/ Total Cost of Ownership
- Infrastructure
- Third-party interactions/interoperability
- Deployment Complexity
- Continual Maintenance
- Procedure & Enforcement
- Lack of automation
- Logging + SIEMs

VERVE

And Threats?

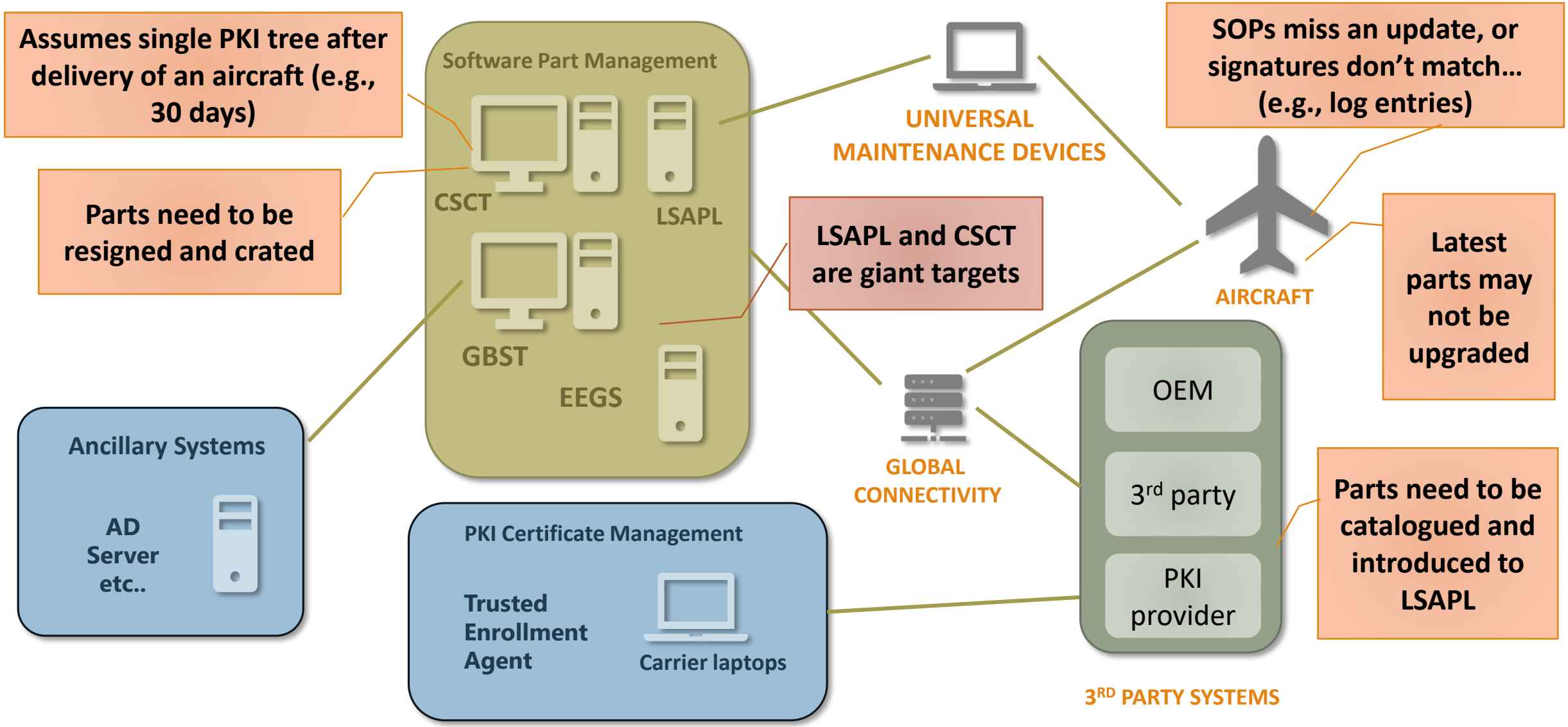
VERVE



And the implementation is also a risk if poorly engineered

Example of Usage for E-Enabled Aircraft by a Carrier

VERVE



And In OT/Critical Infrastructure…

The Scenario of Infrastructure

VERVE

- **Consider the average age** of an industrial facility

- **Asset owners have a non-homogenous environment**
  - Full of vendors, 3rd parties, and tools

- ICS ecosystem is similar to aviation, but

  - **Cryptography/PKI (if it exists) will add work**
  - **Addresses a specific set of issues – e.g., supply chain**
  - **Error handling needs to be graceful – e.g., mismatch, synchronization**

& LSAPs are similar to OT signed firmware …

VERVE

Aviation

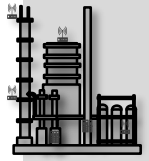
CONFIGURABLE ITEMS & FIRMWARE TRACKING

SUPPLYCHAIN & VENDOR AUTHENTICITY

CENTRALIZED PART MANAGEMENT & FLEET SYNCRONIZATION

AIRCRAFT INTEGRITY & COMPLIANCE

OT



CONFIGURABLE ITEMS & FIRMWARE TRACKING

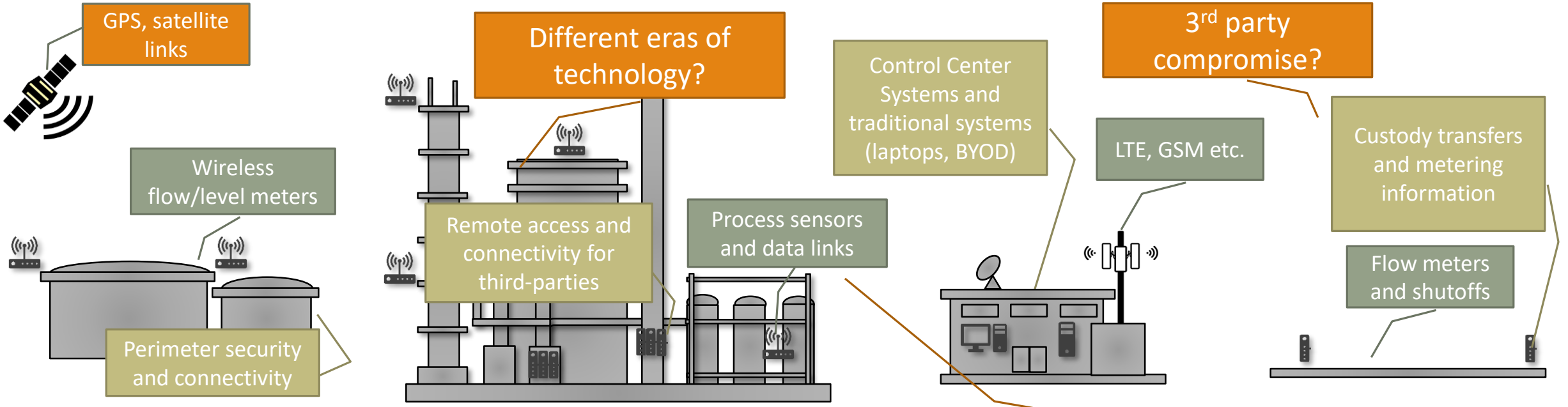
SUPPLYCHAIN & VENDOR AUTHENTICITY

CENTRALIZED PART & SITE INTEGRITY MANAGEMENT

CERTIFICATION AND ATTACK PREVENTION

Airports inherit ICS/OT mappable risks & concerns

VERVE



Safety/OPs vs. Security?

Distributed PKI?

Hash mismatch/certificate expiry?

And the SO What?

VERVE

OT & PKI Issues (The Bad)

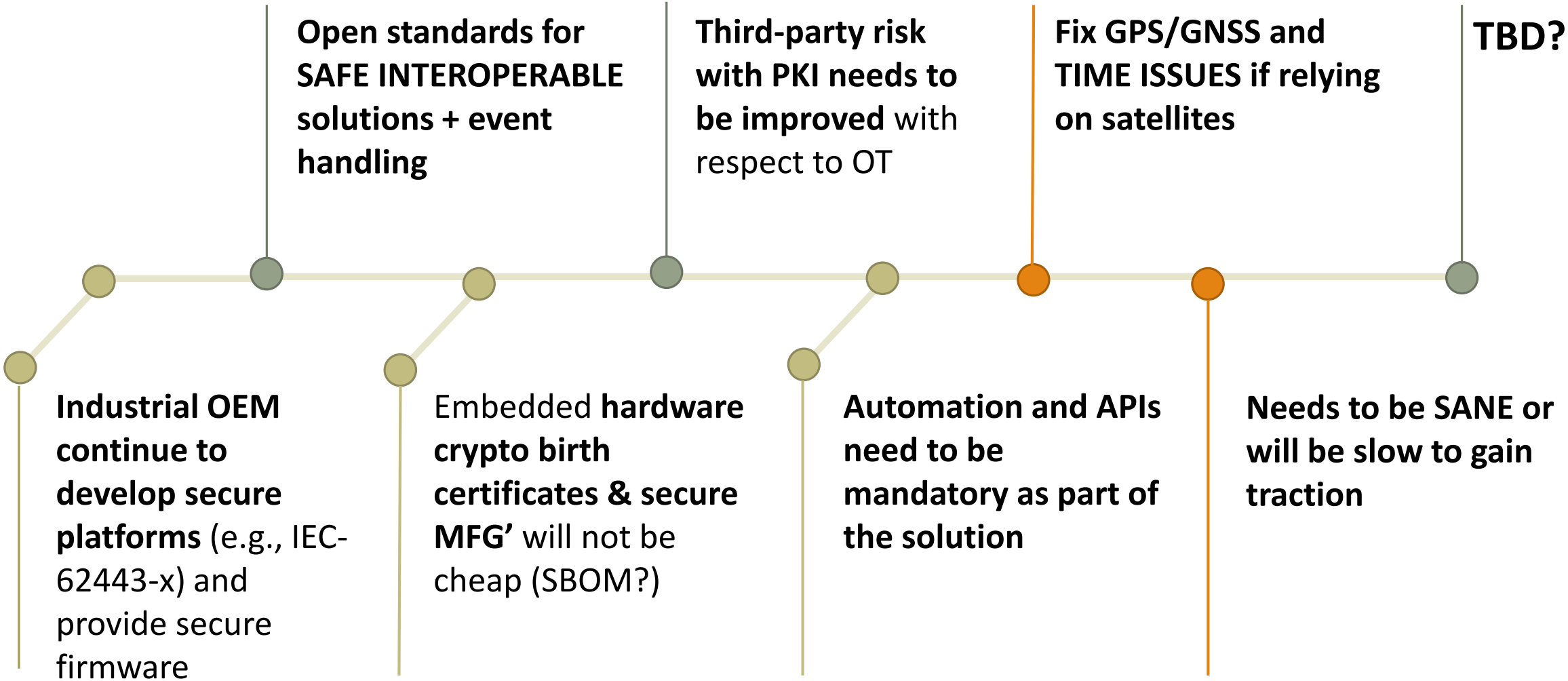
- MFG’ & Delivery challenges
- CRYPTO error handling
- Time/GPS/GNSS dependencies
- Vendor “lock in” may increase
- PKI is just another OT target
- Maintenance – Expiry? Revocation? Apps?
- SOPs for signing/deploying firmware/logic

VERVE

OT & PKI (The Good)

Potential Benefits	Advantages
Asset Reality Synchronization	• Asset inventories will be FORCED to match reality
Code Integrity	• Modifications can be prevented or at least realized assuming PKI is secure
Origin Tracing	• Provides “origin” detection of software • Improves accurate inventory of software + changes
3rd Access Management	• Enable revocation of third-parties access easily
Artefact Controls	• Latest versions of artefacts can be tracked
Forced Vendor Convergence	• Effective asset management will need tie-ins
Opportunity for Automation	• Additional controls for auditing and verification

And to make secure firmware/logic a success…



Ron Brash
Director of Cybersecurity Insights
rbrash@verveindustrial.com

Twitter: https://twitter.com/ron_brash
LinkedIn: https://ca.linkedin.com/in/ronbrash

VERVE

References:

** Noun project for some icons (FOSS)*
** YVR/aircraft images open domain, available from Google, credit to authors, choices where random*
** ARINC/DO-standards from darkweb + google/public sources*

VERVE