



System Security Engineering and Program Protection Case Study for the Materiel Solution Analysis Phase Tutorial Notional Architecture Handout

Melinda Reed

**Office of the Deputy Assistant Secretary of Defense
for Systems Engineering**

**15th Annual NDIA Systems Engineering Conference
San Diego, CA | October 22, 2012**



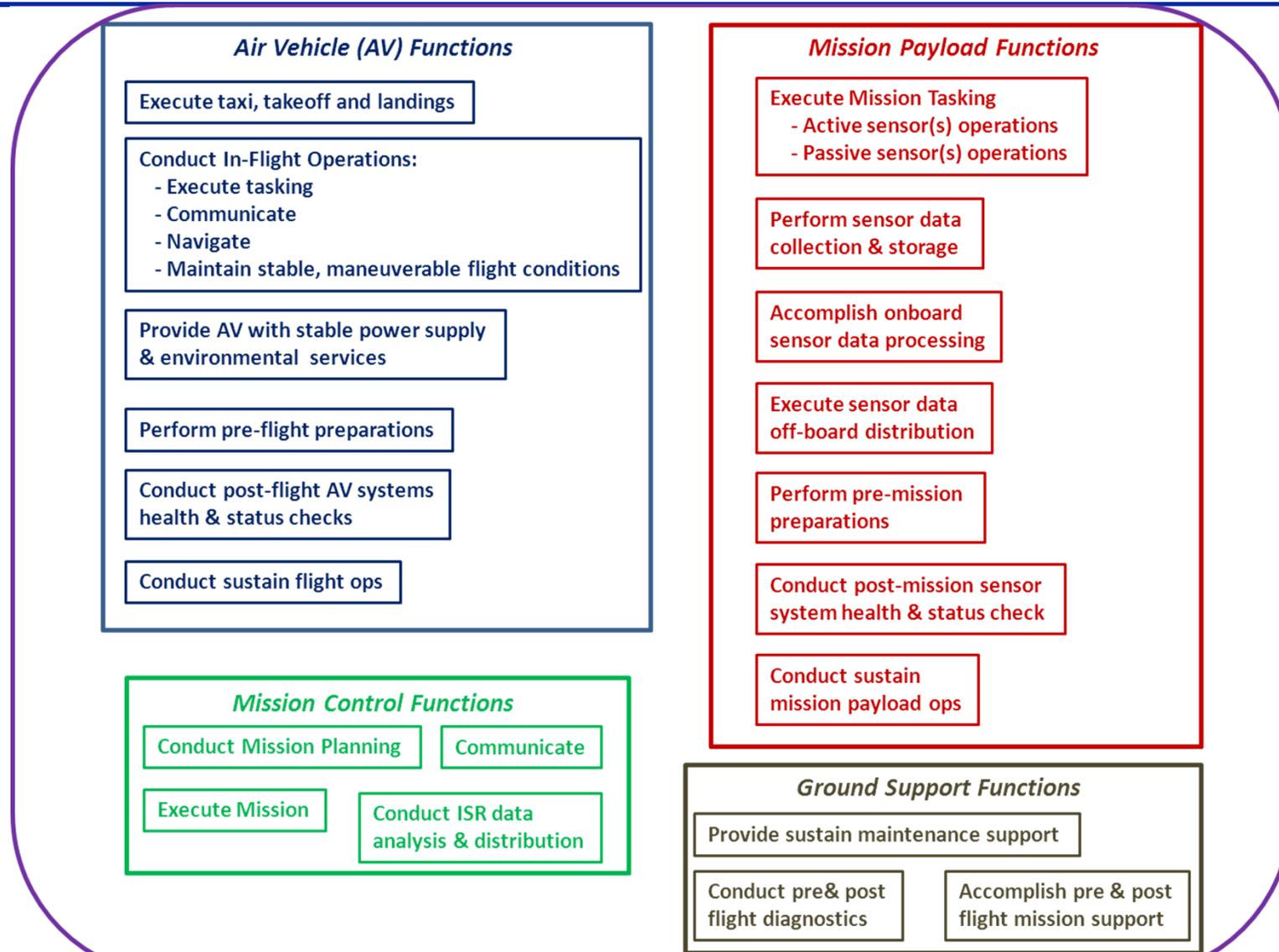
Contents



- **UAV Notional Architecture**
- **UAV Potential Supply Chains**
- **UAV Potential Development Lifecycles**
- **Generic Supply Chain & Malicious Threat Vectors**

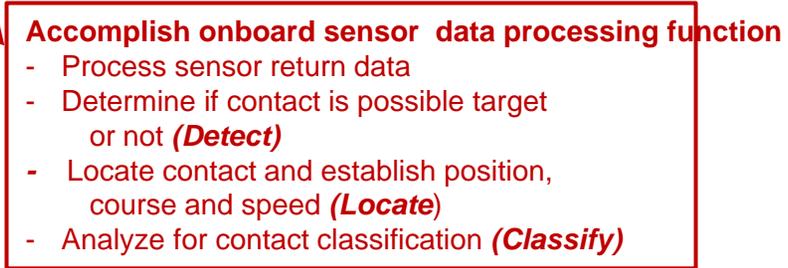
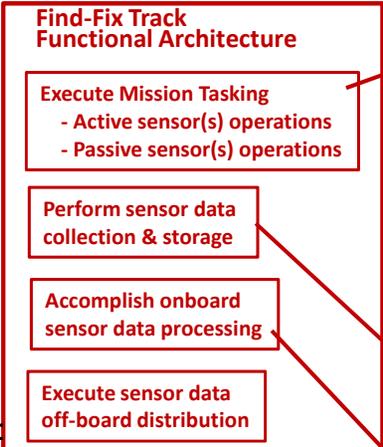
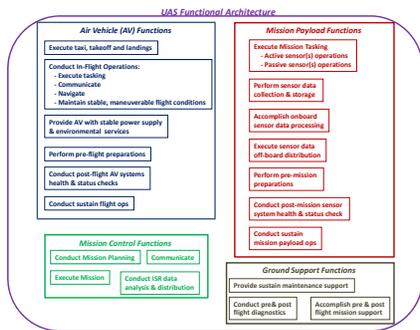


UAS Functional Architecture





Find-Fix-Track Scenario



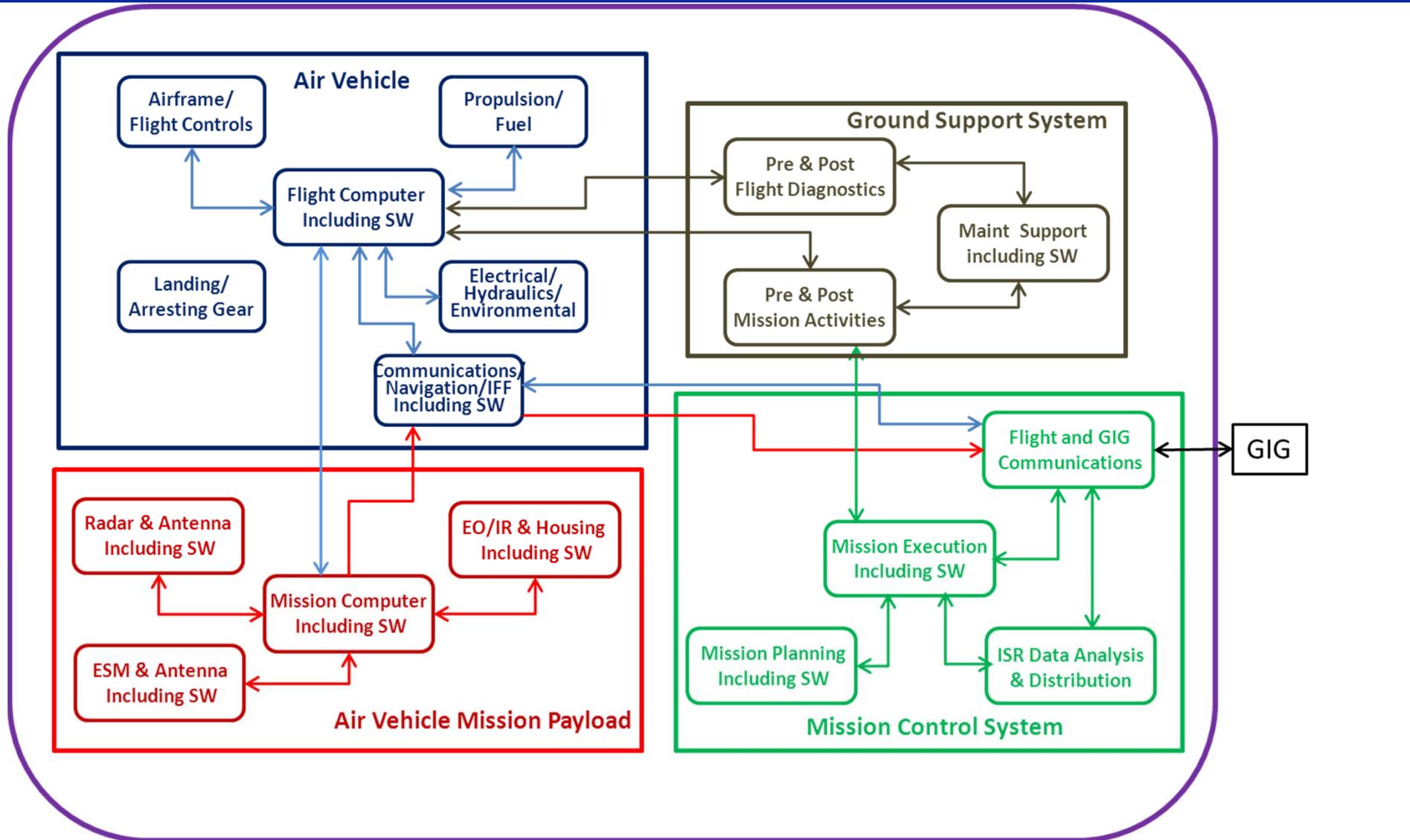
Find, Fix, and Track Functional Order

1. Accept Mission Plan
2. Allocate mission plans to sensors
3. Initiate active sensor search plan (**Search**)
4. Collect and process sensor returns
5. Determine if contact is possible target or not (**Detect**)
6. Locate contact and establish location, course and speed (**Locate**)
7. Position sensor to identify contact with passive sensor(s)
8. Gain passive sensor(s) data and analyze for contact classification (**Classify**)
9. Pass sensor data and analysis results to mission control for confirmation (**Communicate**)
10. Accept tasking to either: 1) initiate track or 2) return to search plan (**Track**)
11. Mission Control tasks return to mission plan execution

Note: Search, Detect, Locate, Classify, Communicate and Track are mission thread functions.

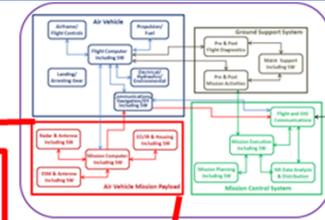
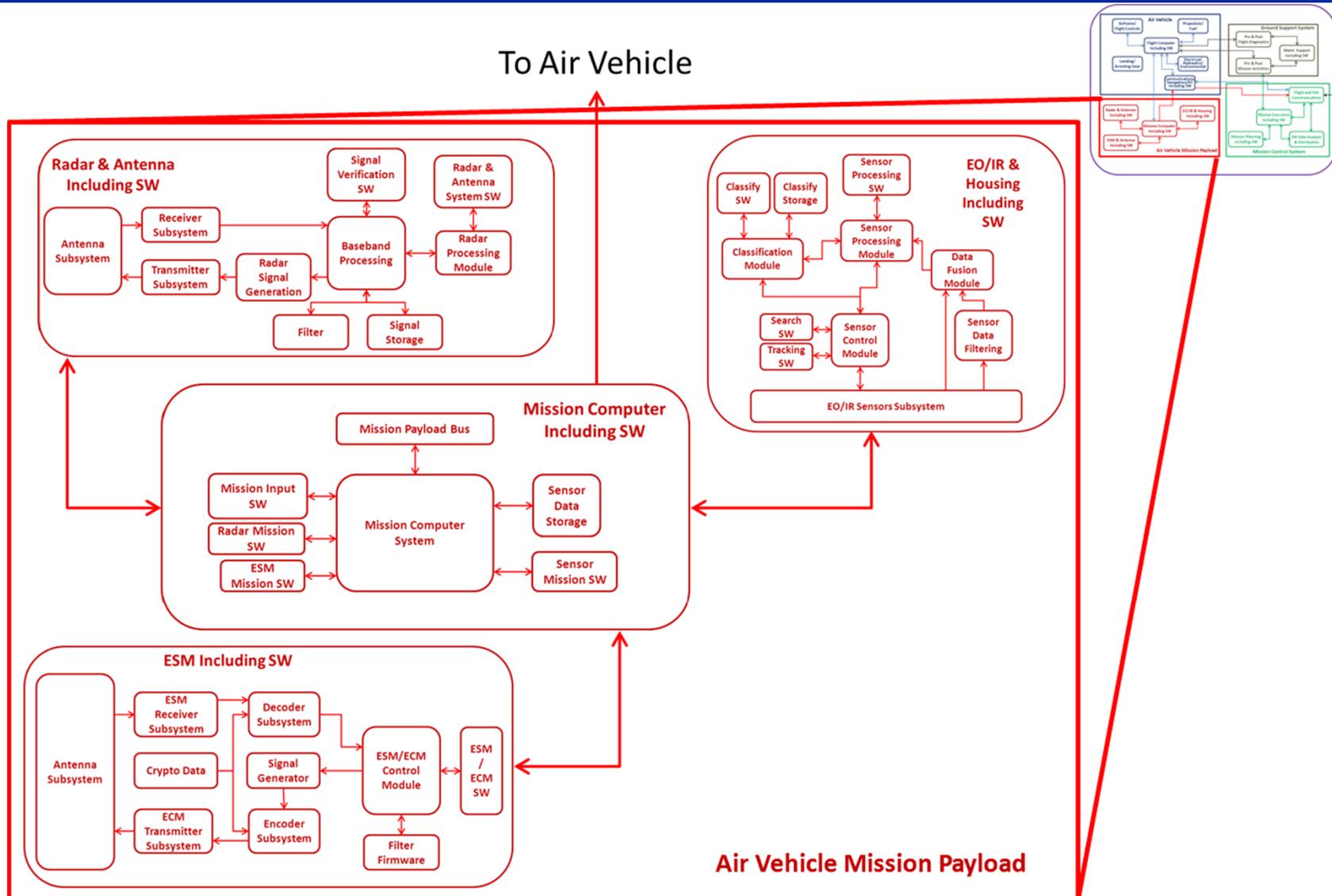


UAS High Level System Design



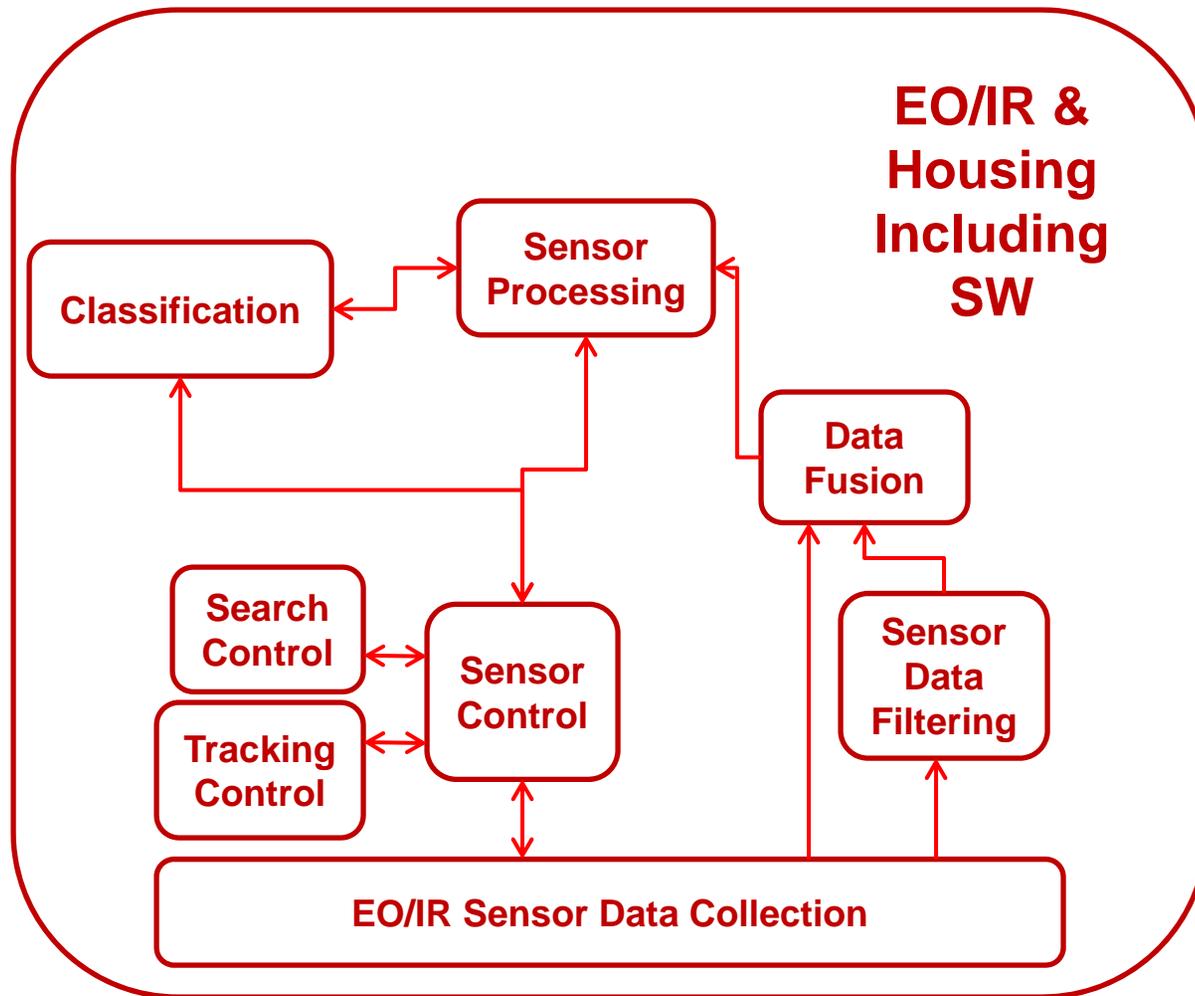


Air Vehicle Mission Payload Diagram



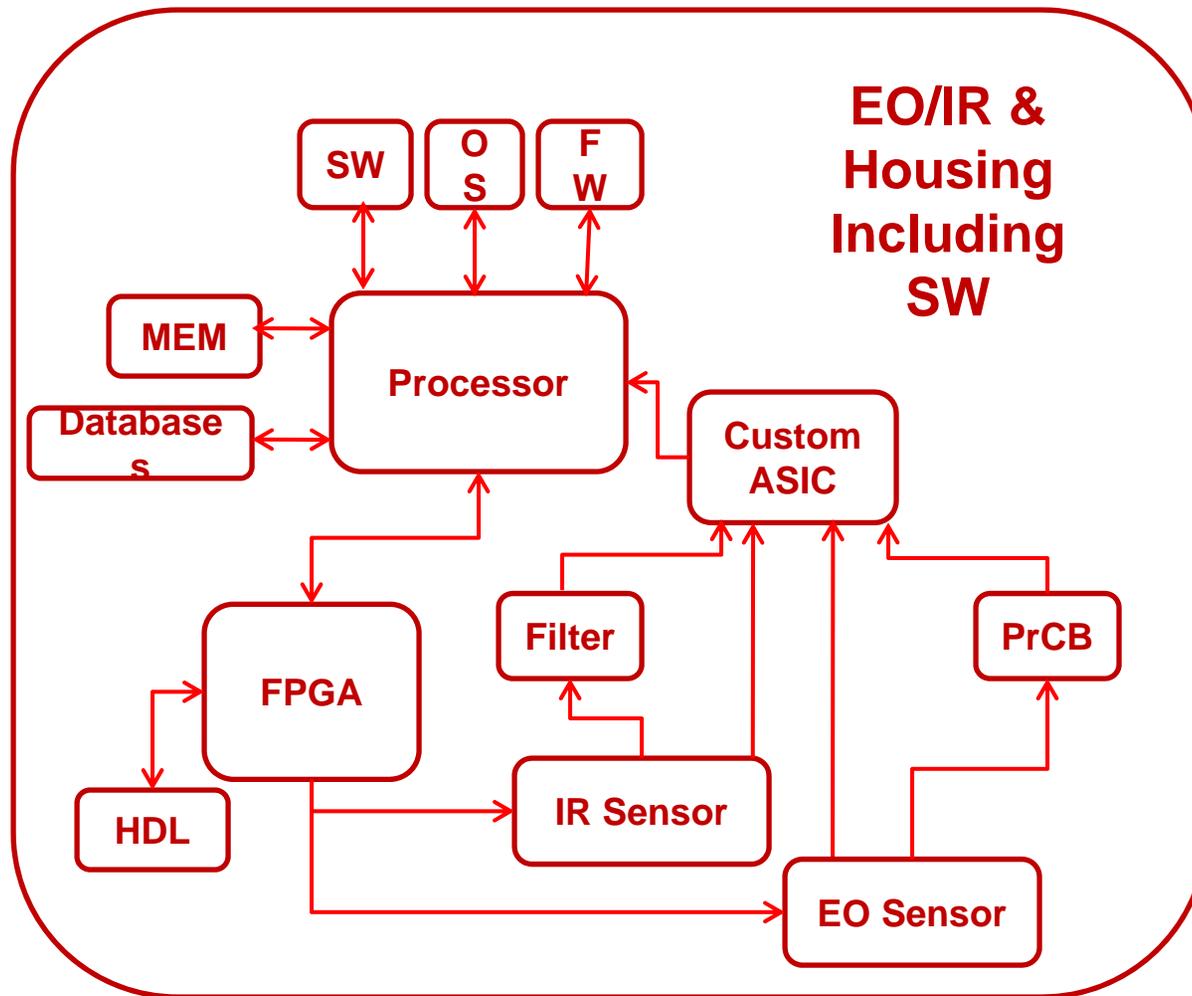


EO/IR & Housing - Functional



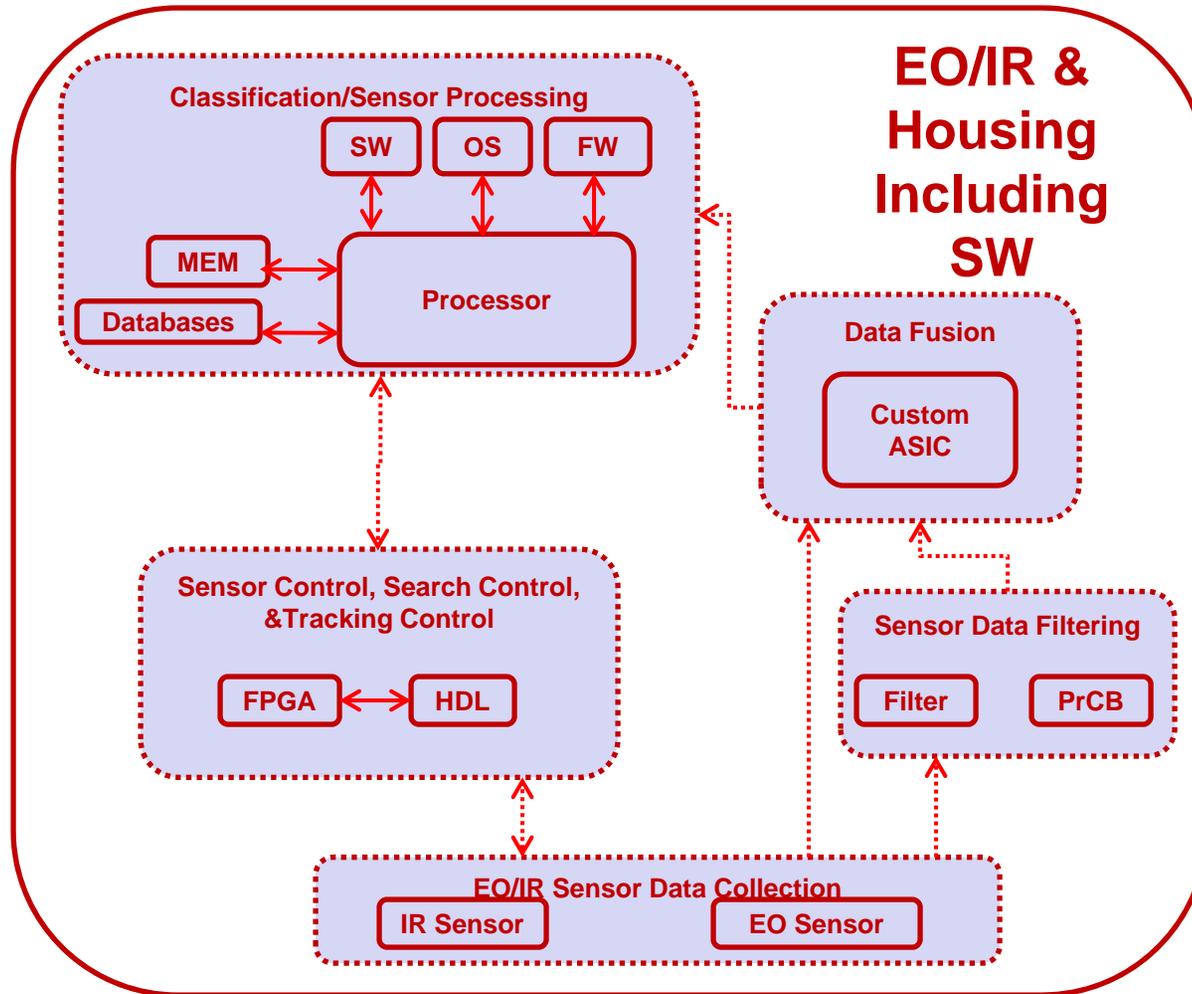


EO/IR & Housing - Physical (supply chain 1)



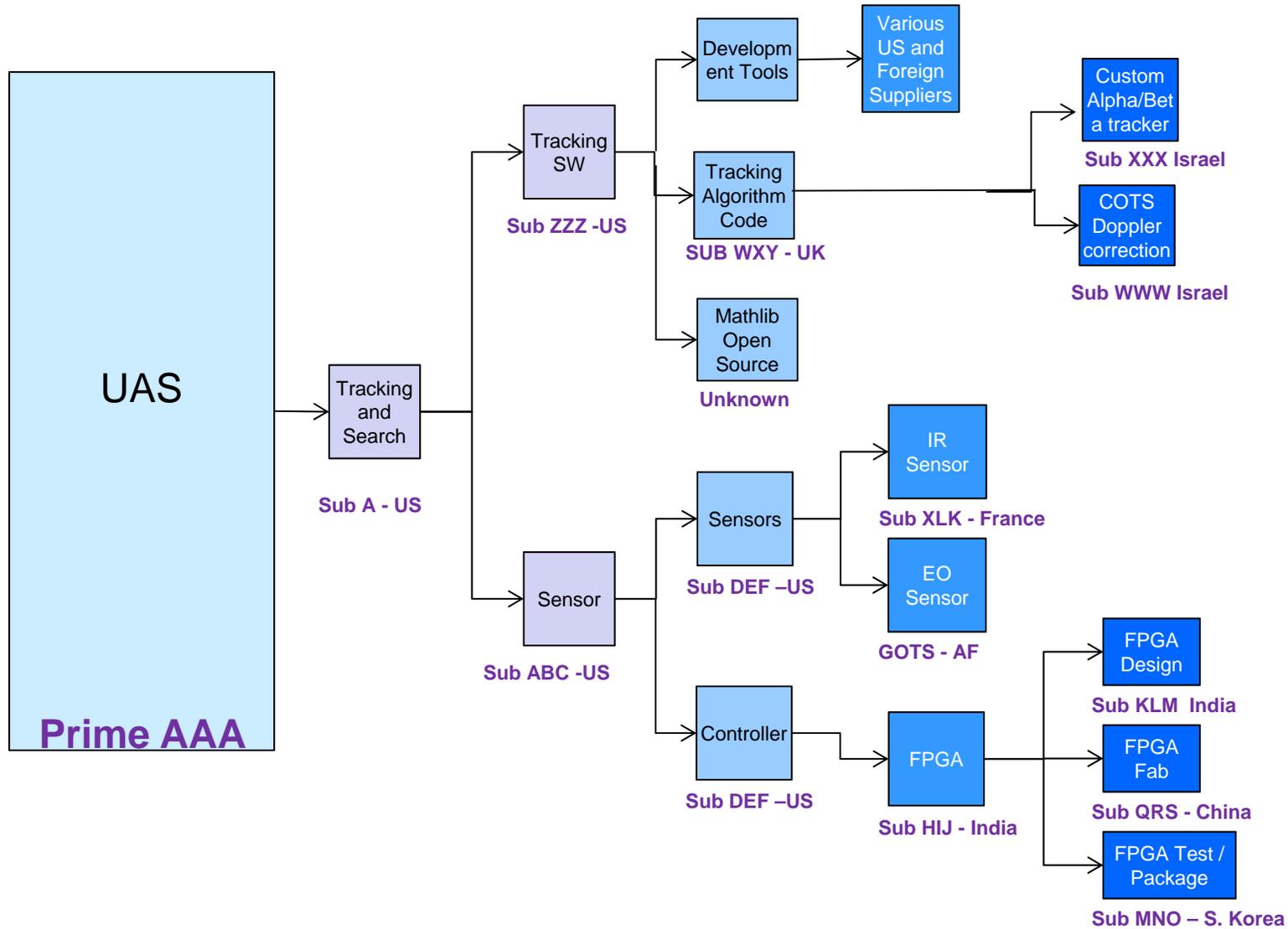


EO/IR & Housing - Allocated (supply chain 1)



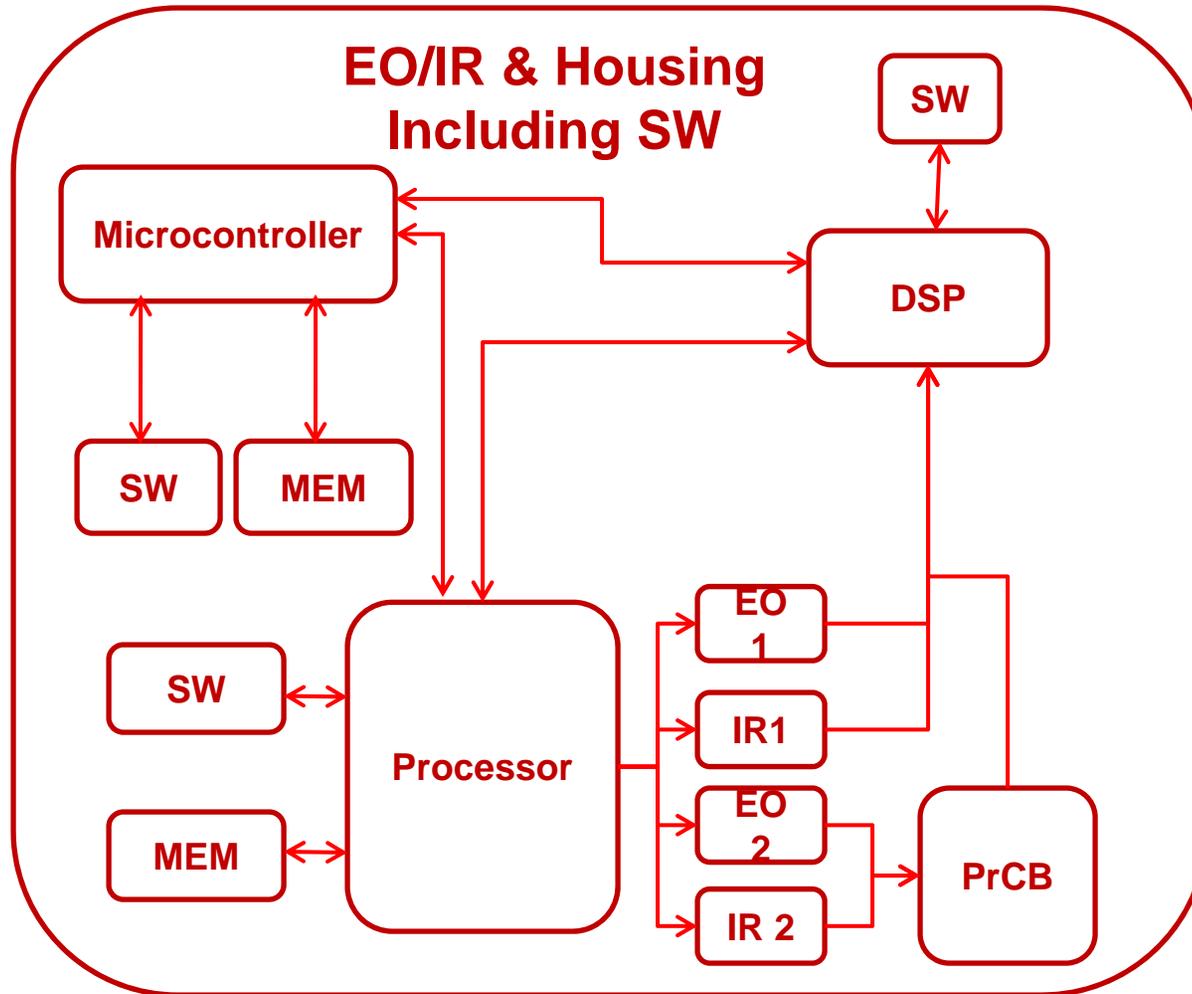


Potential Supply Chain 1



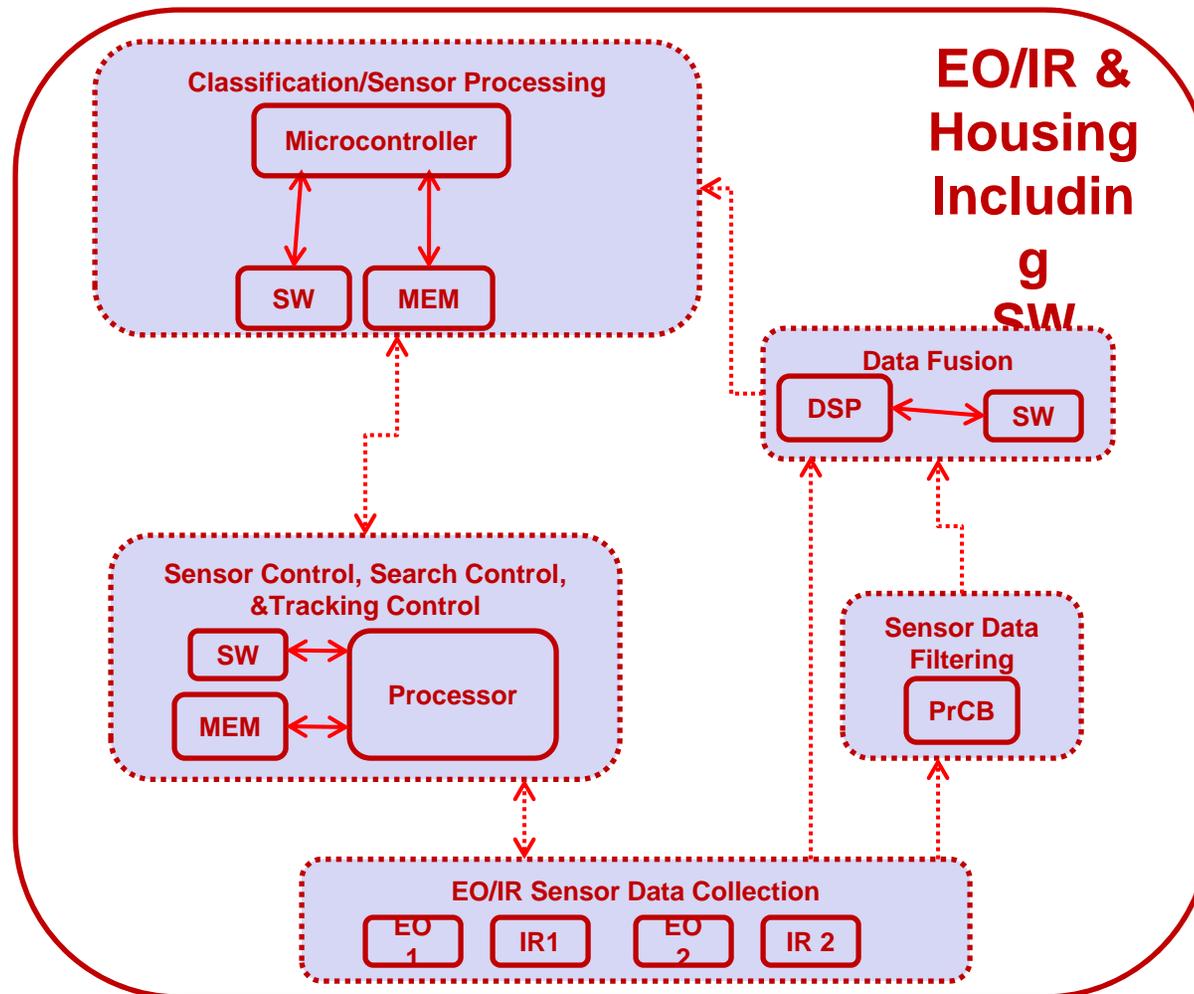


EO/IR & Housing - Physical (supply chain 2)



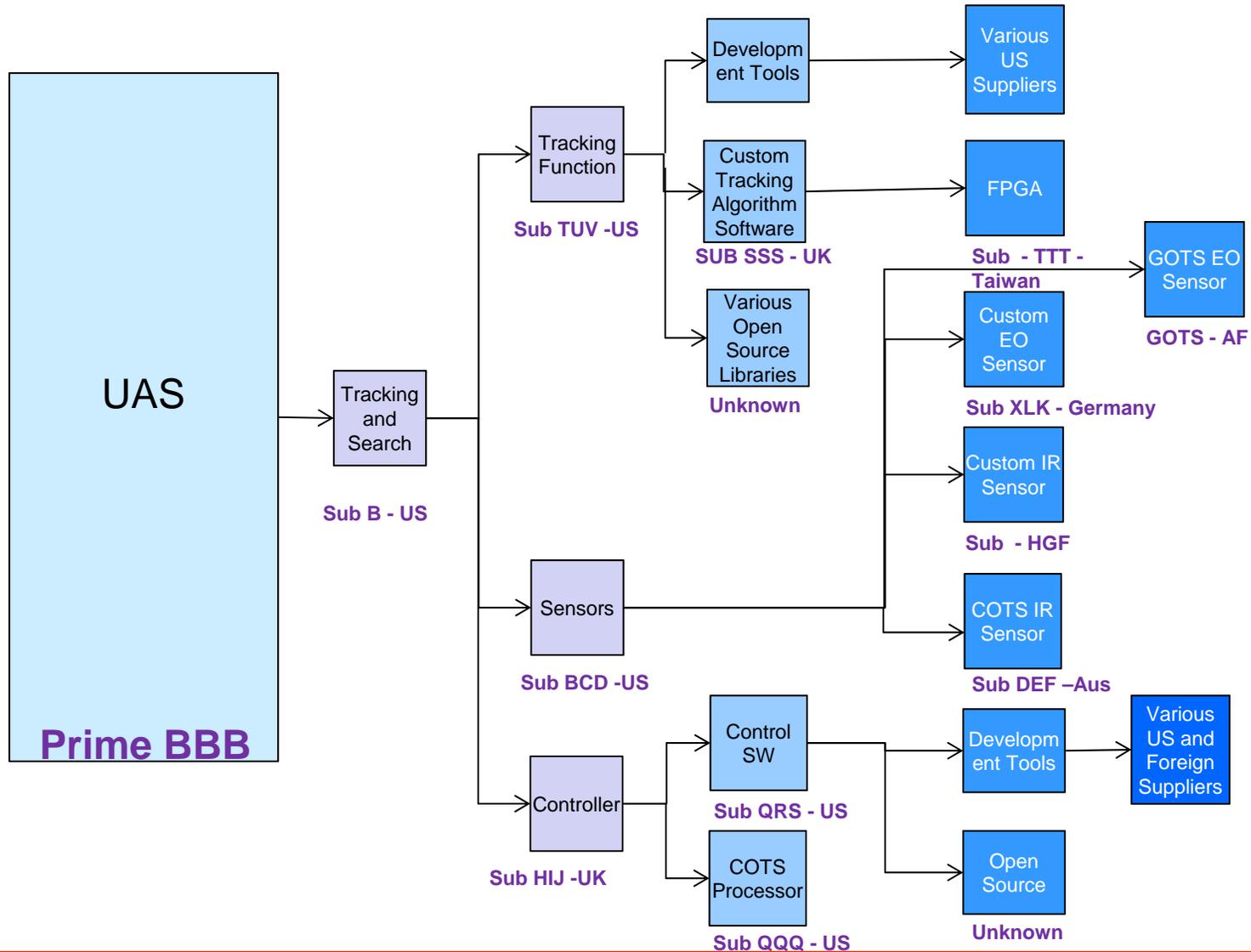


EO/IR & Housing - Allocated (supply chain 2)



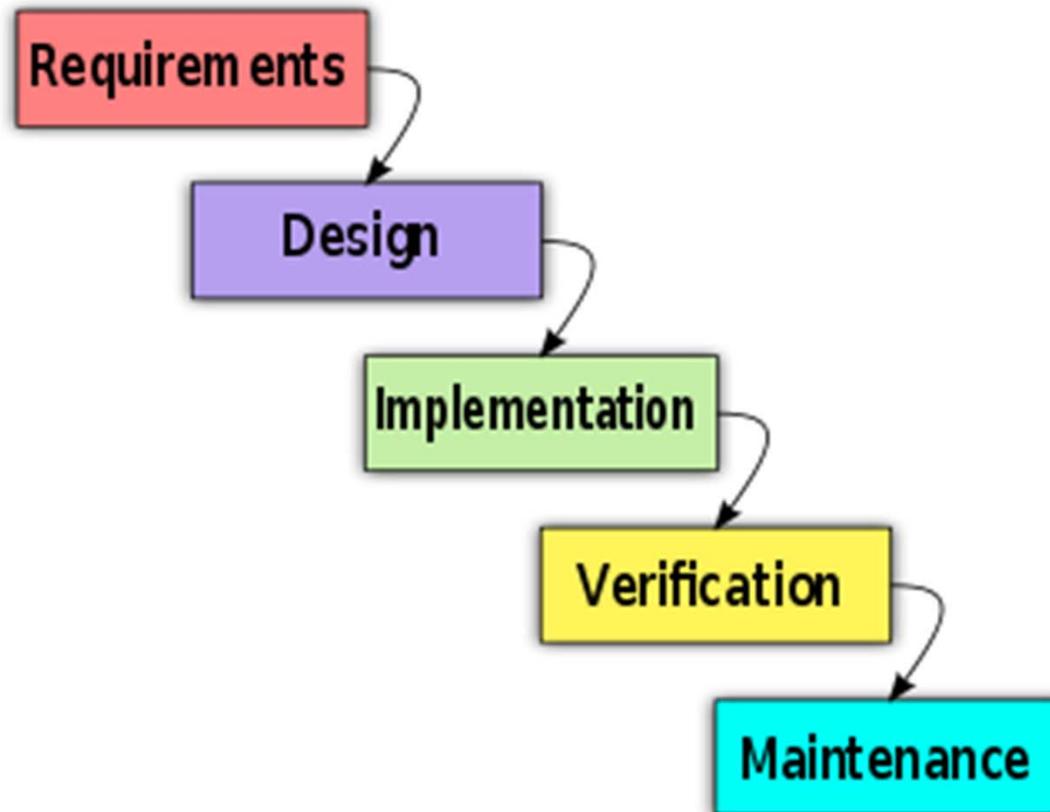


Potential Supply Chain 2



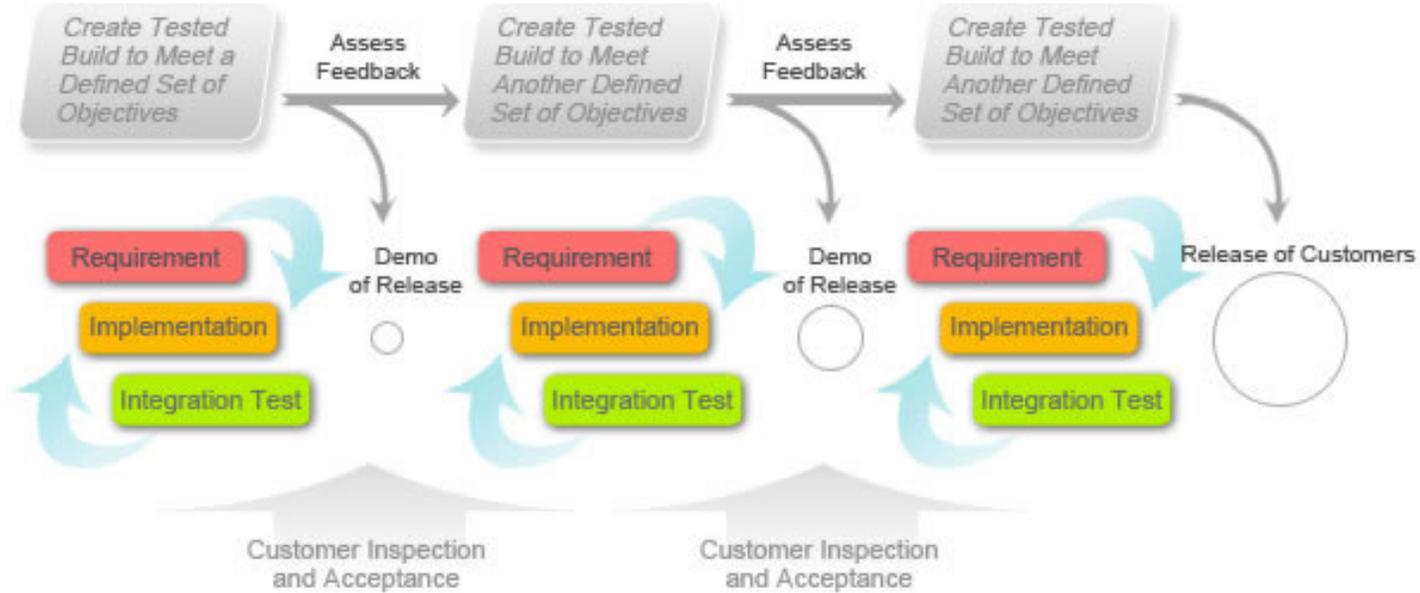


The Traditional (Waterfall) SW Development Lifecycle





Agile Development Lifecycle



<http://www.agilegator.com/pmdevelopment.html>



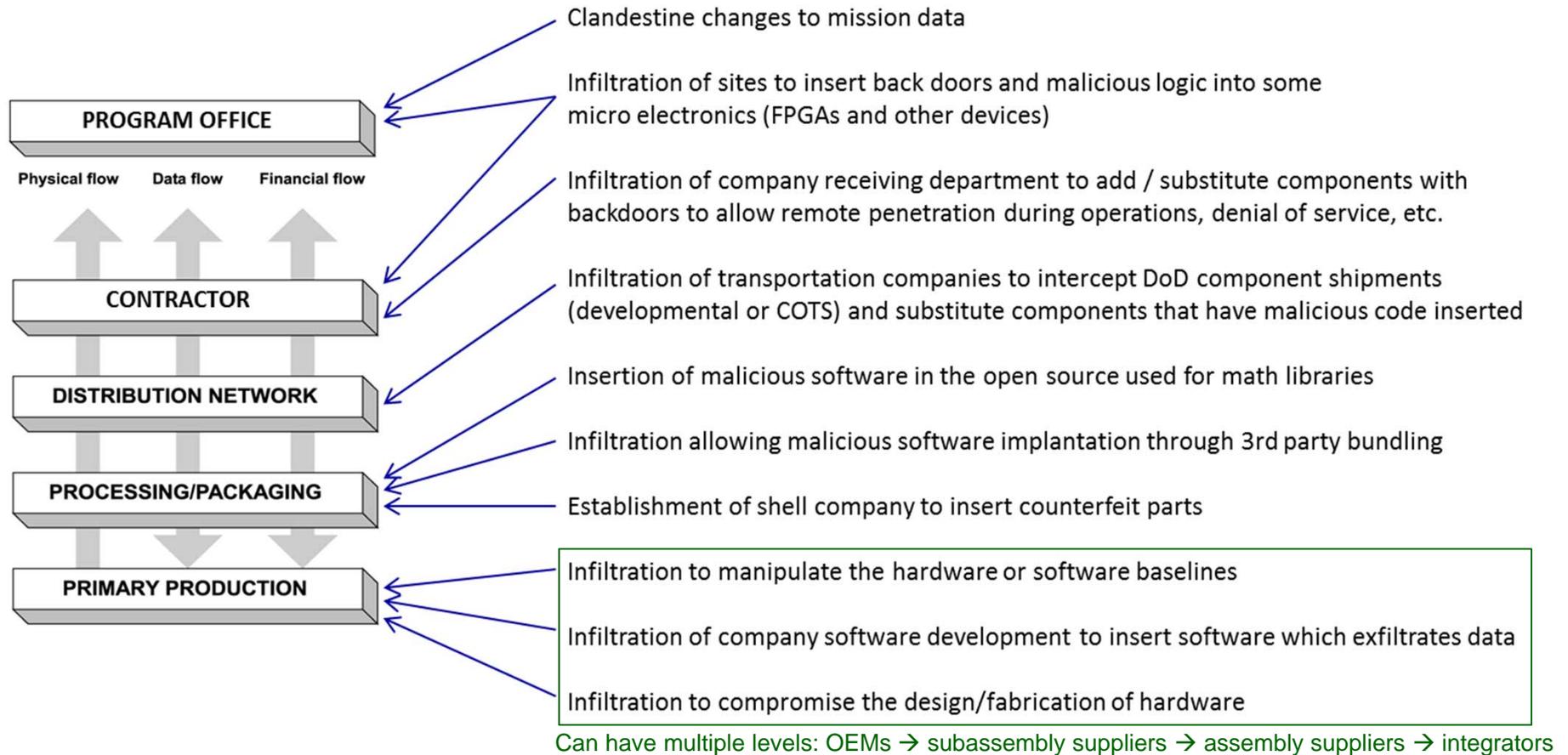
Generic Threats – Supply Chain Attacks



Coverage is for what part of the chain is infiltrated and what the malicious insertion accomplishes

Supply Chain

Attack Vectors





Generic Threats – Malicious System Exploitation Attacks



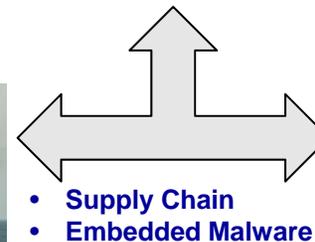
Attack Vectors for Malicious exploitation of fielded systems

Exploitation of system design vulnerabilities



- Configuration, Operational Practices**
- Supply Chain** (penetration, corruption)
- Malware** (downloaded, embedded)
- External Mission Load Compromise**
- DNS Based Threats** (cache poisoning)
- Applications** (built-in malware)
- E-mail Based Threats** (attachments)
- Data Leakage** (via social media)
- Password Misuse** (sharing)

- Denial of Service** (embedded malware)
- Kill Switch Activation** (embedded malware)
- Mission Critical Function Alteration** (embedded malware)
- Exfiltration** (by adversary)
- Network Threat Activity** (host discovery)
- Compromised Server Attacks** (on clients)
- Malicious Activity** (disruption, destruction)
- Auditing Circumvention** (evading detection)
- Web Based Threats** (disclosing sensitive info)
- Zero Day Vectors** (vulnerabilities without fixes)
- Improper File/Folder Access** (misconfiguration)

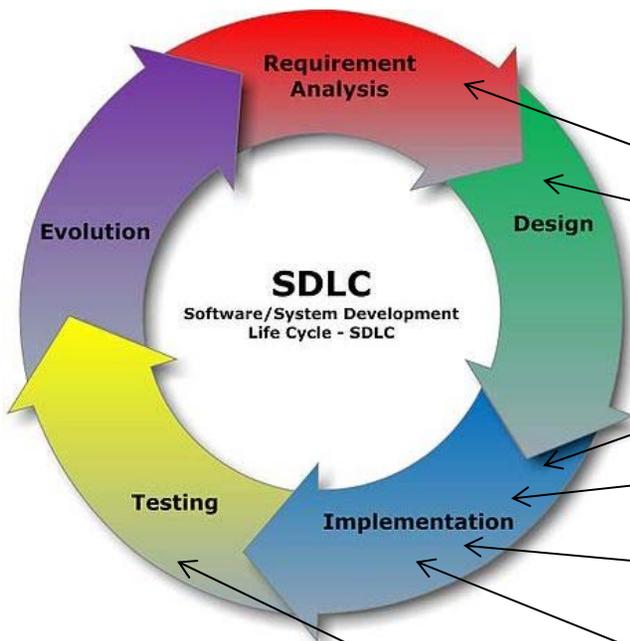




Generic Threats – Software Development Life Cycle Malicious Insertion



Coverage is for what part of SDLC is targeted and how malicious insertion is accomplished



Attack Vectors for Malicious Code Insertion

- Hidden in software's design (or even requirements)
- Appended to legitimate software code
- Added to linked library functions
- Added to installation programs, plug-ins, device drivers, or other support programs
- Integrated into development tools (e.g., compiler generates malicious code)
- Inserted via tools during system test