



Towards a Safe & Reliable Operation of Cyber Physical Systems

02 Feb 11

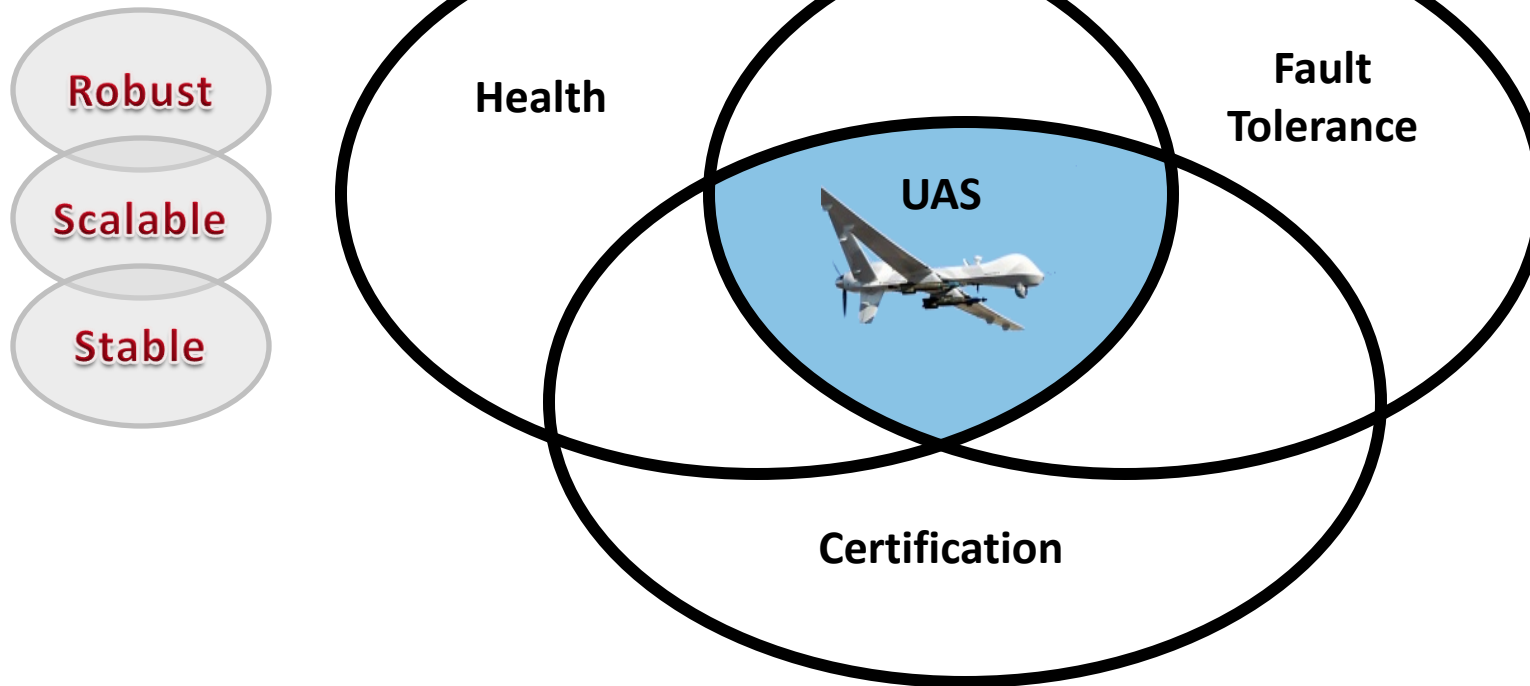


**Ken Eizenga
Air Vehicles Directorate
Air Force Research Laboratory**



Overview

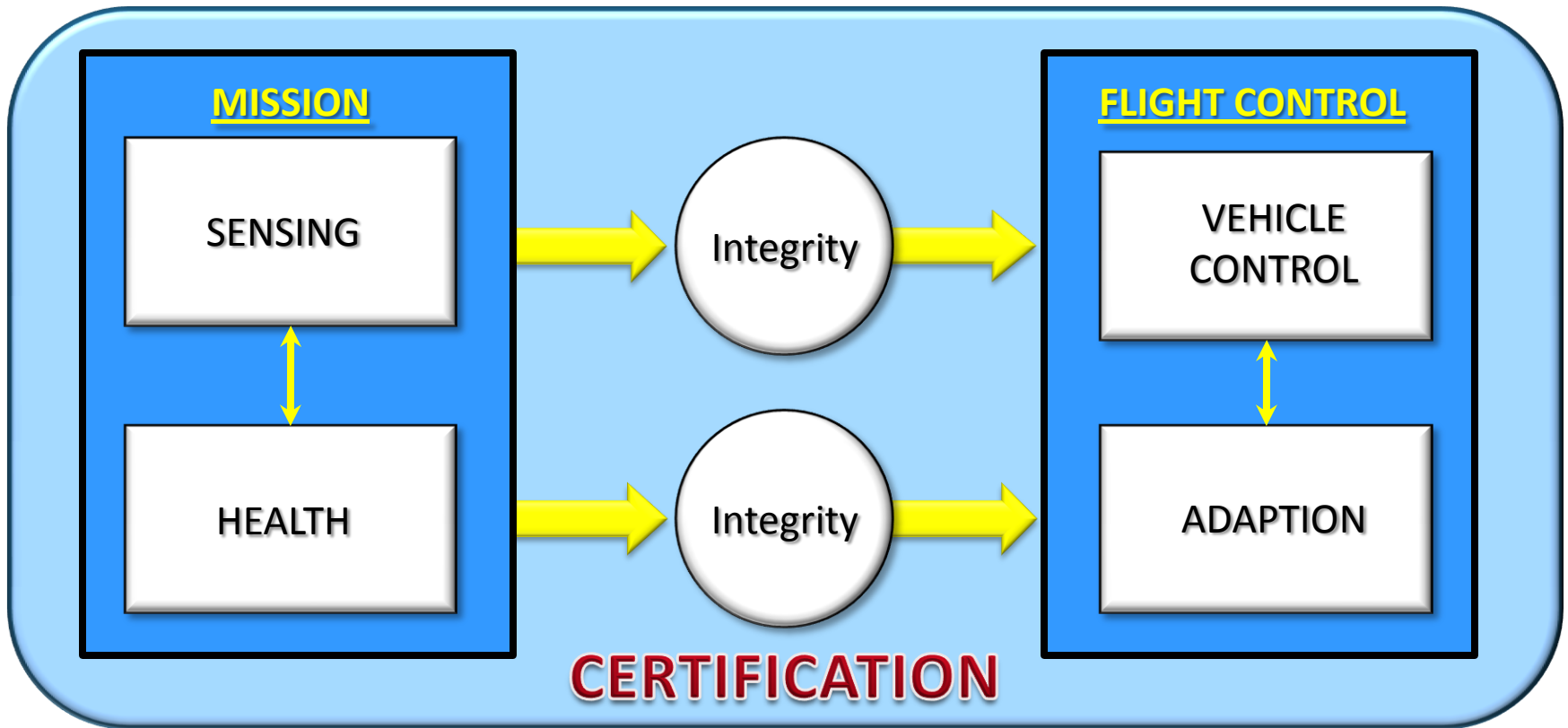
Cyber Physical Systems



CHALLENGE: An autonomous air vehicle / system (UAS) **MUST** maintain a high level of Safety



An Integrated Approach to CPS



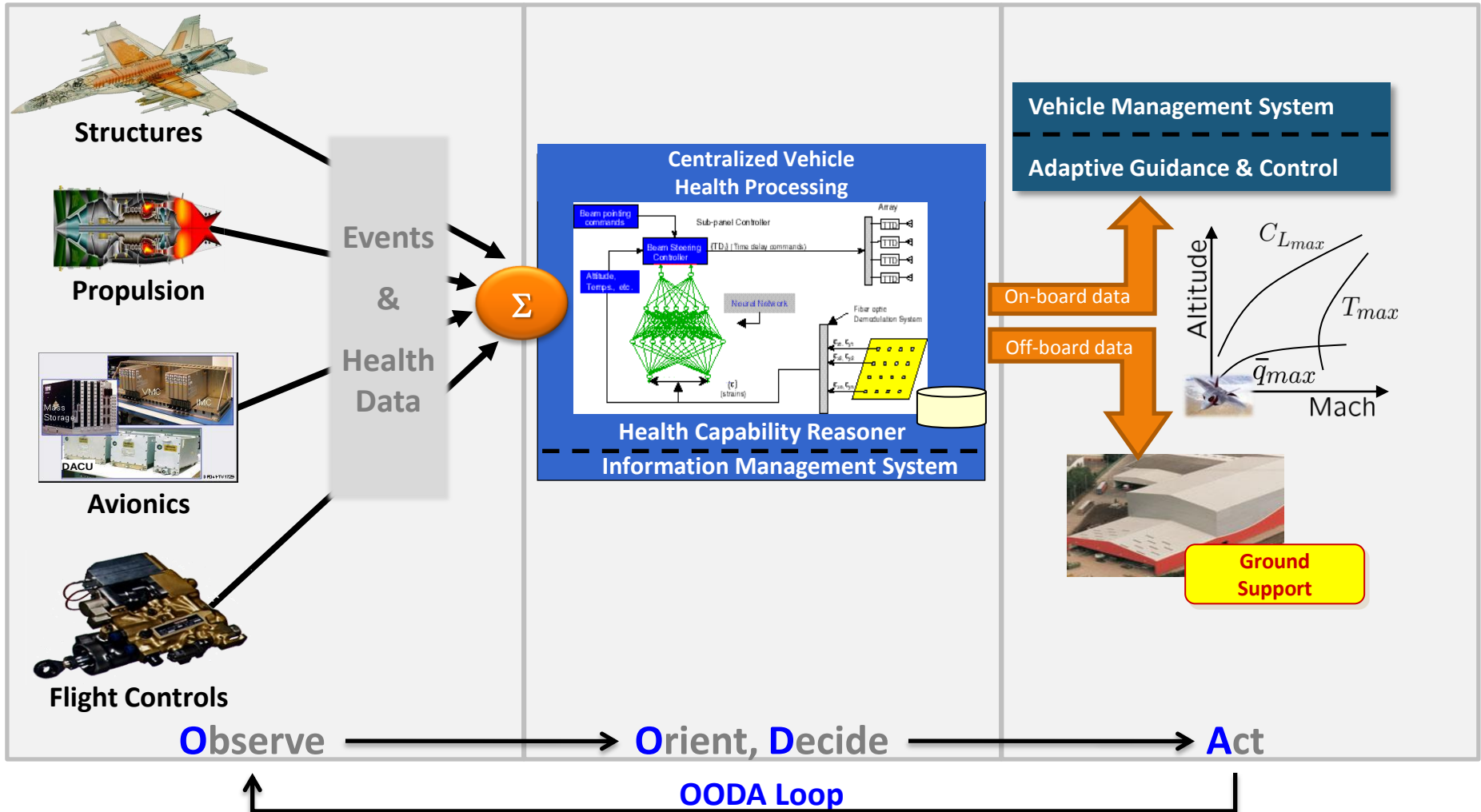
Certifying a CPS that includes:

- Integrated System Health Management (ISHM)
- Adaptive Guidance & Control (AG&C)



ISHM Architecture Approach

ISHM: Detect Damage, Assess Damage, Determine Ability to Perform Mission





ISHM Technical Challenges



- Determine the current health capability of the vehicle through the onboard, real-time analysis of sensor information
- Implement performance constraints for real-time mission management
- Integration of mixed criticality systems
- Specifying ISHM requirements for early design cycle and systems engineering involvement to ensure system integrity and design for integration

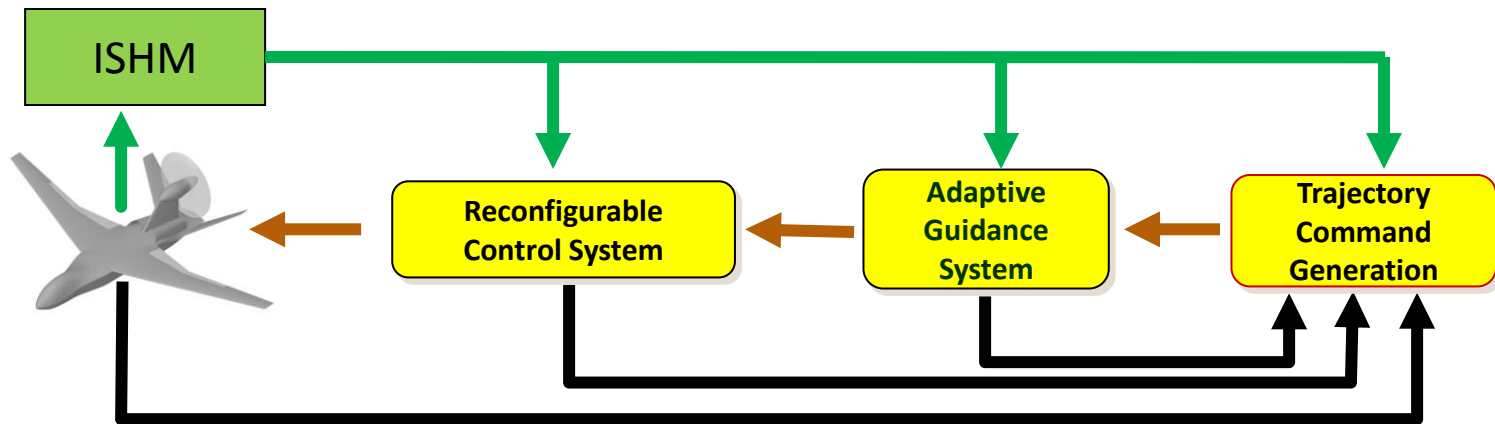


Adaptive Guidance & Control (AG&C)

AG&C Definition

- A flight control algorithm that stabilizes and controls the flight vehicle in real time in accordance to its updated health capabilities
- Uses ISHM real-time outputs
- Modifies actuator commands and flight trajectory according to its health capabilities to enhance safe operation in the event of failures

AG&C Approach





AG&C Technical Challenges



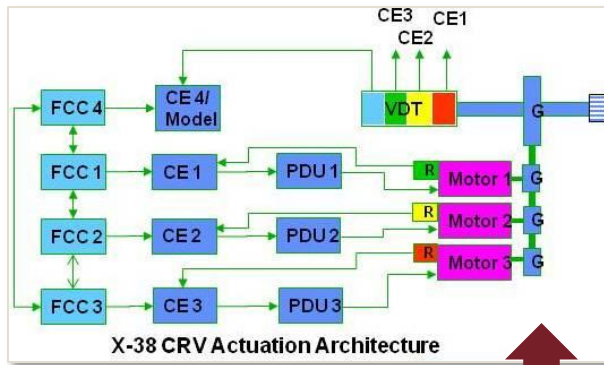
Technical Challenges

- Real-time modeling of vehicle dynamics under failures and degradation
- Real-time computation of vehicle constraints and flyable envelope
- Full envelope, integrated adaptive guidance and control law for all flight segments
- Verification, validation, certification of an adaptive, reconfigurable guidance and control algorithms



ISHM-AG&C Application

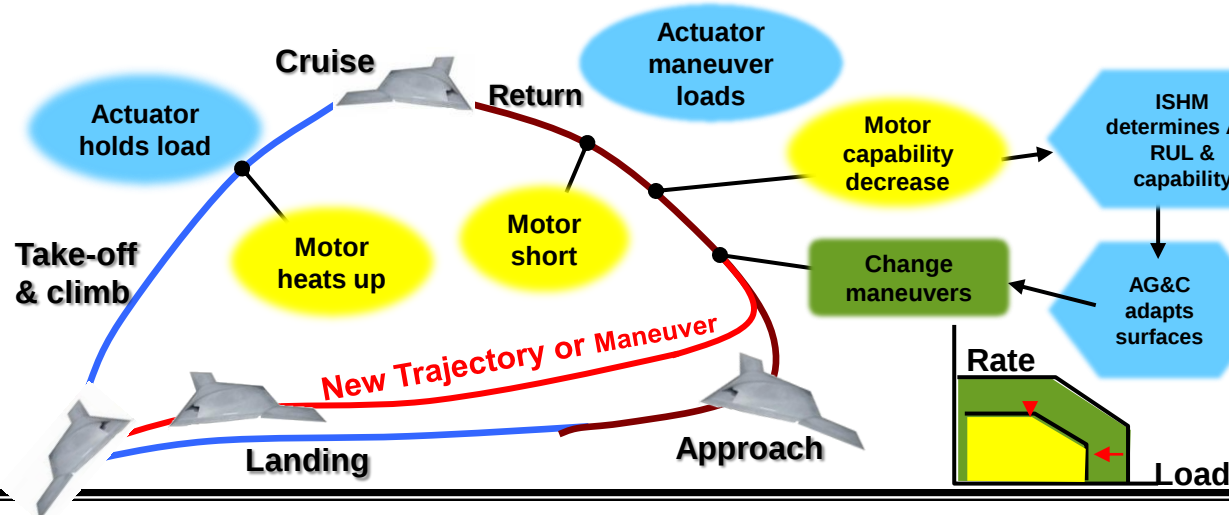
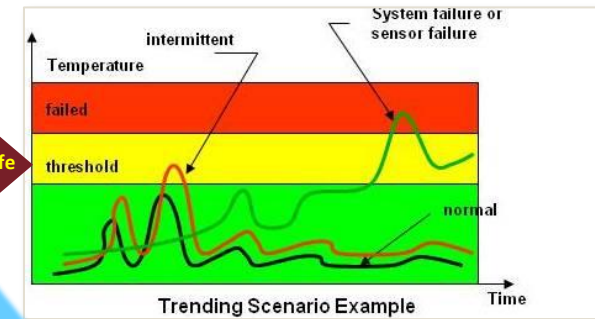
Objective: Utilize Health Diagnosis for Real-Time Fault Tolerance to Enable Continued Mission Op's



VMS/AG&C/IMS
Health Reasoner

Monitors Components

Detects Failures & Projects Remaining Life



Triggers Flight Control Adaptation



Designing for Certification...



Focus Areas...as applied to ISHM

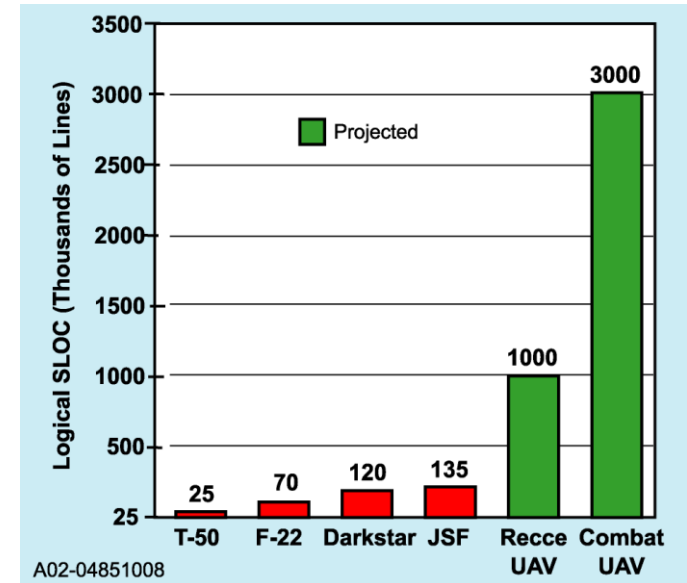
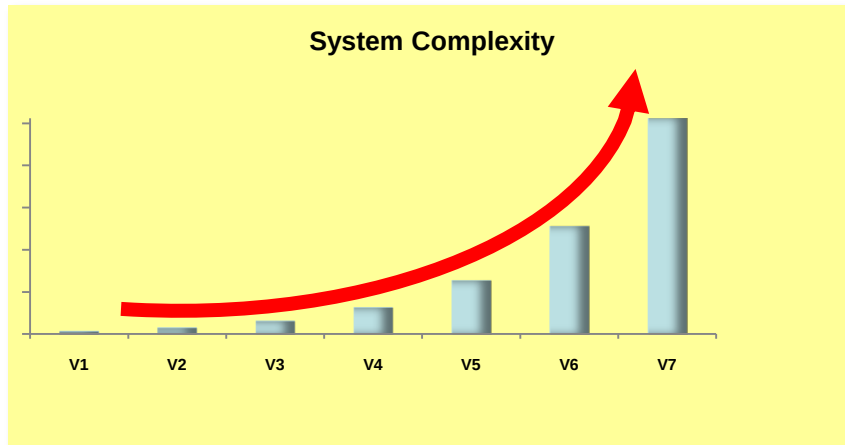
- Composable Architecture
 - Modular, pre-certified building blocks to increase reuse and speed up design
- System Partitioning
 - Time and space separated software and data with explicit and well-defined communication between partitions
- Advanced Analysis Techniques
 - Formalize design requirements to facilitate the use of formal methods and code analyzers
- Integrity Management
 - Analytical redundancy to determine soundness of data from sensors and subsystems



Challenges in Certification



Non-determinism drives Complexity Explosion



As applied to ISHM

- Proving the reliability/correctness of data from sensors and subsystems
- Trusting the decision on performance capabilities of system by algorithms
- Proving the system latency will not impact vehicle safety

As applied to AG&C

- Proving stability margins for attitude after control change
- Proving convergence time to allow for real-time, safe adaptation



Summary



✓ Health

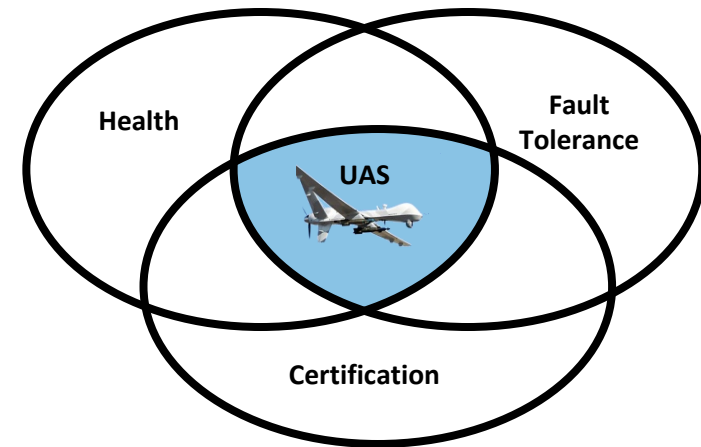
- ISHM allows us to know the current health status of the system and predict future health status

✓ Fault Tolerance

- Subsystems can utilize ISHM data to adapt in real-time to failures and changing conditions

✓ Certification

- Certification enables trust in safe, adaptable systems



**An autonomous Cyber Physical System
MUST
maintain a high level of Safety**



Upcoming Events

- **Safe & Secure Systems & Software Symposium (S5)**

- Dates: 14-16 June 2011
- Place: Dayton, OH
- Save the date email sent in Jan



- **ISHM Conference**

- Dates: 19-21 Jul 11
- Place: TBD (likely Boston)





Contacts



- **ISHM**

- Ken Eizenga, 937-255-6290

- Kenneth.Eizenga@wpafb.af.mil

- J.B. Schroeder (*ISHM Conf*), 937-255-8431

- John.Schroeder@wpafb.af.mil

- **AG&C**

- Dr. Anhtuan Ngo, 937-255-8439

- Anhtuan.Ngo@wpafb.af.mil

- **Design for Certification**

- Russ Urzi (*S5 Symposium*), 937-255-8294

- Russell.Urzi@wpafb.af.mil