


**Designing Future Systems for
Airworthiness Certification**

**A Look at Mixed Critical
Architecture Requirements
(MCAR)**

DAVID HOMAN, Technical Area Leader
Control Systems Development and Applications
Air Vehicles Directorate
AFRL/RBCC


David B. Homan, Technical Area Leader
Flight Critical Systems and Software Certification
Control Systems Development and Applications Branch
2130 Eighth St.
Wright Patterson Air Force Base, OH 45433-7542
David.homan@wpafb.af.mil
(937) 255-4026

Russell E. Urzi, Technical Program Manager
Control Systems Development and Applications Branch
2130 Eighth St.
Wright Patterson Air Force Base, OH 45433-7542
Russell.urzi@wpafb.af.mil
(937) 255-8294

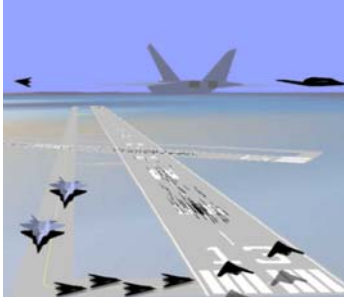





Mixed Critical Architecture Requirements

Cooperative Airspace Integration Technology Goals



Same Base, Same Time, Same Tempo




- **Mixed Manned/Unmanned Teams**
- **UAV In-situ Decision Making**
- **Transparent Airspace Ops**
- **Adaptive Software V&V**
- **Reliable Unmanned Ops**

Based on JUCAS ICD, SAB Summer Study, Global Hawk ORD, OSD UAV Roadmap, Predator CCD

Cooperative Airspace Operations (CAO) will develop and demonstrate key onboard and offboard control technologies that enable effective and responsive utilization of unmanned systems as applied in a system-of-systems construct in dynamic mission environments. The technologies are grouped into two attribute areas: collaborative teaming of UAVs with manned and unmanned systems; and safe interoperable, autonomous airspace and ground operations. The former emphasizes cooperative/collaborative behaviors that enable multiple vehicles to perform as a cohesive, effective unit, with performance as a primary driver. The latter emphasizes safe operation of unmanned systems in proximity of other manned and unmanned systems, whether on the ground or in the air. A necessary component of both attributes therefore is autonomy: the ability of an individual vehicle system to successfully complete a wide variety of complex missions requiring numerous decisions that demand consideration of many factors, in difficult physical and tactical environments with minimal human oversight. This includes the ability to not only calculate the best route to accomplish objectives, but the ability to determine the goals to be met and to manage resources. Additionally these unmanned systems are not to operate separately from the rest of the battlespace. Groups of unmanned and manned vehicle systems must have the ability to jointly plan and successfully execute complex missions with minimal human oversight as a default, but still allow the operator to interact as desired. This will require additional capability on- and offboard in order to generate and maintain operator situational awareness such that they remain an integral and effective part of the system. Finally, UAVs will need to operate safely in and around airbase, other aircraft, and terrain. Collision avoidance is a critical capability for the success of UAVs, especially in complex environments such as the terminal area or for urban applications.


The Air Force Research Laboratory, Air Vehicles Directorate (AFRL/RB) has S&T activities to investigate more autonomous use of UAVs, in particular for use as a strike capability that assists or replaces manned air vehicles in these high risk and dangerous missions. Under its new capability-focused technology initiative, AFRL/VA has identified Cooperative Airspace Operations (CAO) capability to address development, maturation, demonstration, and transition of critical on-vehicle control technologies to enable UAVs to perform missions effectively in a complex and dynamic battle space environment. In addition, these new UAV platforms will need to be capable of safe interoperation and collaboration with manned and unmanned assets within a system of systems strike architecture.

The key attributes of the CAO capability are: operations in manned and unmanned teams; safe operations from airbases and in airspace; and the flexibility to be as autonomous as needed, and as interactive as desired to contribute to the mission at hand. Progression of the CAO capability will lead to an ultimate vision of "Same Base, Same Time, and Same Tempo", i.e. UAV's become an integral, seamless, and highly effective component within the Air Force arsenal.




Mixed Critical Architecture Requirements


Enabling Technology for Full Capability Utilization of UAVs




Mixed Criticality: Mission & Flight




Authority Mgmt: Autonomy-Autonomy




Mixed Initiative: Man-Autonomy



Future UAV Functionality Outdate Current V&V And Certification Process

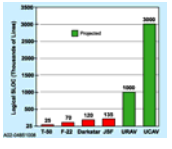


On Board Situational Awareness & Contingency Management



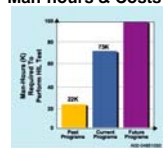
Advances in V&V and Certification Enable Intelligent – Autonomous UAV Control Systems

Unmanageable # of Lines of Code




System	Lines of Code
F-16	~100,000
F-22	~200,000
Darkstar JSP	~300,000
UAV	~500,000

Increases in Test Time, Man-hours & Costs



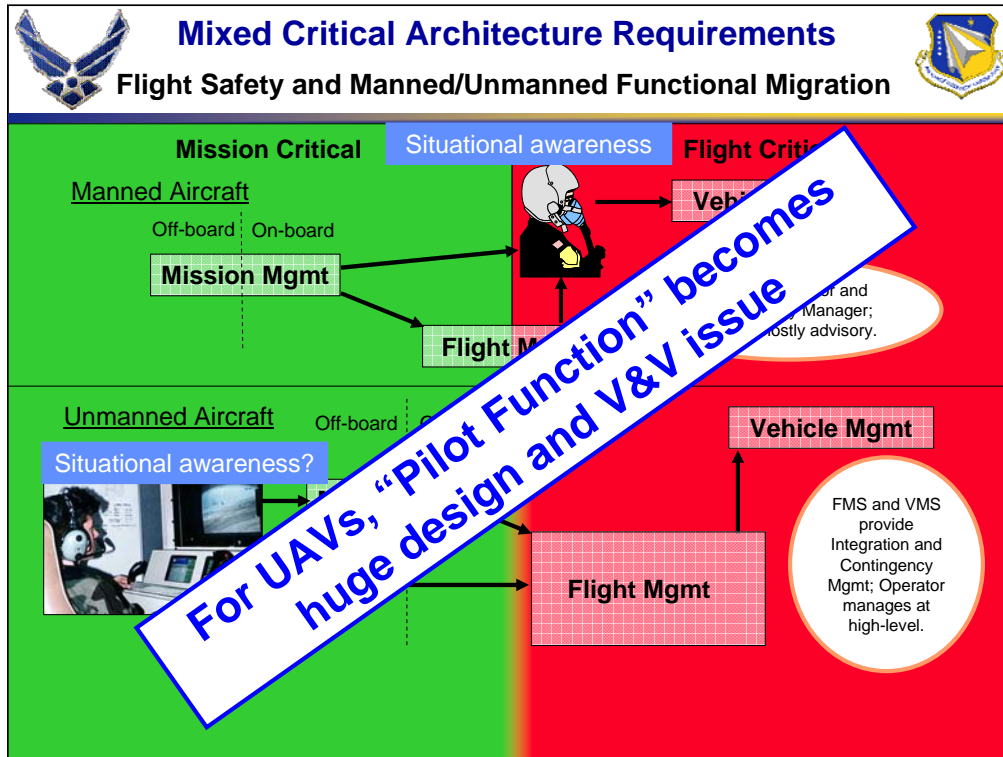
Program	Man-hours (Millions)
Test Program	~10
Current Program	~30
Future Program	~50

V&V dominant driver

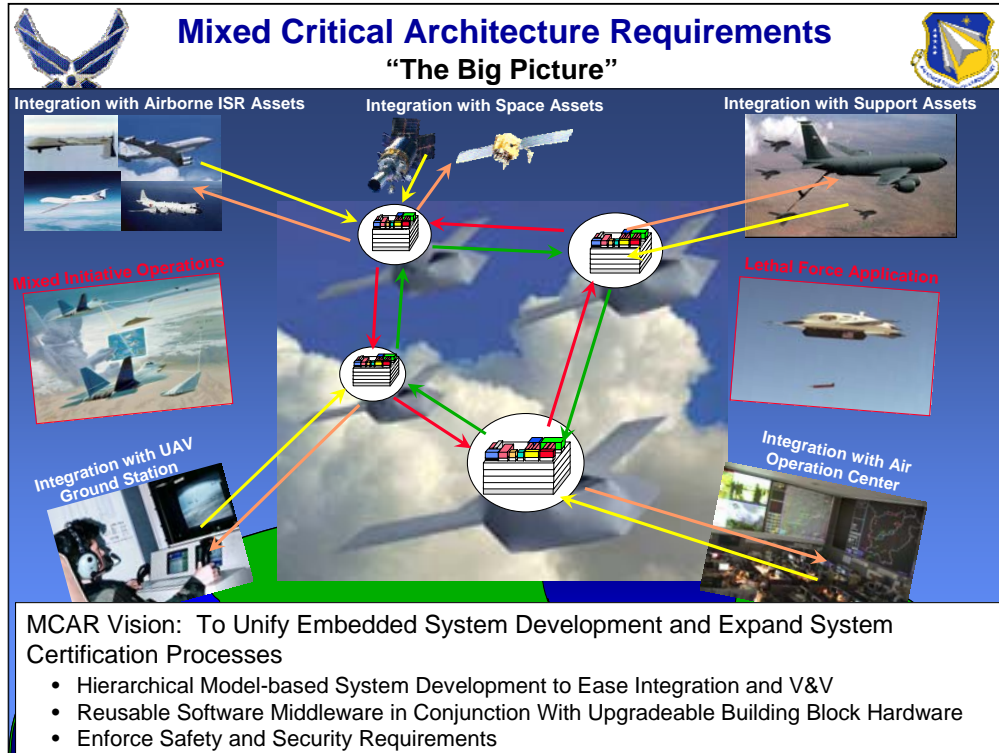


Category	Percentage
Other	20%
Test	25%
V&V	35%
Control	20%

As the Air Force works toward developing intelligent and autonomous weapon systems, a daunting task looms. How can we certify that a decision-making intelligent system is safe when the decisions are unpredictable? Trusting decisions made by autonomous control software will require completely new methods and processes to guarantee safety. The difficulty lies in determining how these intelligent systems will operate in a dynamic environment and with less human oversight. New paradigms will be needed to assure safety. Certification of flight control technologies is already the most rigorous testing embedded computer systems endure. Intelligent control adds a whole new dimension of issues. Adding intelligence can be divided into three challenges: building intelligence, instilling safety, and enabling affordability. All three are closely related. Cost and safety issues will influence how we design and build intelligence. UAV autonomous control is a revolutionary leap in technology. Such control replaces decision-making that required years of training for human operators. Neglecting autonomous control certification research today will dramatically increase tomorrow's cost of ownership for future users. Future Air Force systems are being planned to operate with minimal human oversight. In this case, new paradigms will be needed for airworthiness certification of these systems to provide the necessary assurance and confidence that all flight critical safety requirements have been met, while using a timely and affordable certification process. Computer systems have already replaced many of the menial human tasks, such as throttle control, automatic lights, and pinpoint targeting systems. Control systems to execute higher order and more complicated functions, such as autopilots and unstable flight modes, are considered mature technologies. However, future Air Force systems are being designed to include autonomous features, such as: automated mission planning, target selection and mission re-planning; multi-vehicle cooperative control; battle damage reconfigurable control; integrated active control with diagnostic and prognostic health systems; aerial refueling; and operation in and around airports. As the control system scope increases, the inherent difficulty in number of lines of code, V&V, and testing skyrockets. Some key technology issues surrounding UAV autonomy include: a mixed-criticality systems architecture, adaptive and learning systems with multi-modal functionality, mixed initiative and authority management and interaction (human-autonomy or autonomy-autonomy); multi-entity systems capability for functions that encompass multiple platforms, and sensor fusion integration that delivers sensor-derived information at high confidence levels. For autonomous control systems to meet these capabilities, software will experience a significant growth in the number of lines of code, with some estimation to be 500,000 to 1,000,000 lines. Current validation and verification processes will become obsolete to certify these systems based upon the sizable costs in time and resources needed to certify the software, and managing the complexity of these systems designs



Autonomous control is a revolutionary leap in technology. Such control replaces decision-making that requires years of training for pilots, or in the case of UAVs, remotely located operators. In piloted systems, we as designers take advantage of the human ability to deal with uncertainty, to be able to make decisions with incomplete or ambiguous information, and to provide the “outer-loop” control input that manages any contingency while maintaining stability and control. The machine itself remains completely deterministic. Future UAV systems will be designed to make their own common sense decisions and judgments. In order to trust decisions made by an autonomous system, it is envisioned new methods for control software verification and validation will be required for airworthiness certification of the control software. At first glance, autonomous systems may appear to be an evolutionary step in control technology; however, it is possible these systems will include non-deterministic functionality. Just as different pilots may make different decisions under the same conditions, autonomous computer control may not be completely predictable. The difficulty will be in certifying the safety and effectiveness of these intelligent systems and determining how they will operate in a dynamic environment. Part of the desire for intelligent control is to be able to react to unplanned events. The problem is testing for all possible outcomes. If all potential events cannot be predicted, then there is no contingency to test for all potential events. In the end, how does one know the reaction is appropriate?



MCAR Program Objective: is to create a compose-able architecture where safety and security are assumed system characteristics. Most safety-critical systems have the same attributes: most are time-critical, most are fault tolerant/redundant, and most provide data/system integrity. Some of these attributes are shared with security. These attributes can be built into an “open” architecture that can be utilized across various applications. This architecture could also include a “cyber-segregation”, where non-critical and safety-critical systems could safely and efficiently utilize the same computational resources.

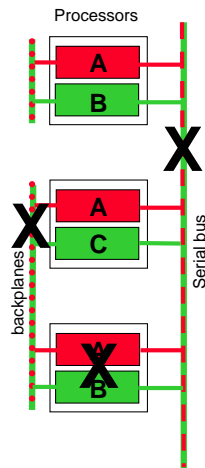
MCAR Program Approach: currently, a layered software approach is being considered, consisting of a high confidence Real-Time Operating System (HC-RTOS) and Flight Management System specific Middleware. The HC-RTOS provides the foundation for the architecture, providing the low-level fault tolerance and separation support for safety and security applications. The HC-RTOS would also be required to perform the priority-based scheduling that would assure the execution of safety-critical functionality and would perform exception handling should the non-critical functions over-utilize the resources. A hybrid scheduler could be used to provide static scheduling for safety critical functions and allow dynamic scheduling for non-critical functions. Memory partitioning would be managed by the HC-RTOS and intrusions would be handled as exceptions that would have implications to the Middleware-layer. Isolation services (such as watchdog timer) would be implemented in this layer to provide the capability for fault containment. The domain-specific Middleware Layer would provide the higher-level execution scheduling and services for distributed processing and communication with other entities. Implementation of redundancy and security management would occur in this layer. Scheduling deconfliction of



Mixed Critical Architecture Requirements



Mixed Criticality Challenge



How can we separate the mission and flight critical functionality as to guarantee safety?

SOA: Middleware that provides time/space partitioning (ARINC 653).

Issue:

Both Criticalities use common HW resources (i.e. processors, backplanes, busses etc); how do we determine PLOC and fault tolerance?

- Understand failure mechanisms for partitioning
- Non-critical function must not take out shared resources...Or the probability of its occurrence is predictable...
- Need guarantee on fault tolerance

Answer may reside in a SW/HW architecture specifically designed for mixed operation

Mixed Criticality: In order to optimize weight/volume for UAV systems, it is tempting to mix mission and flight critical functionality within the same computation platform. For manned systems, this would warrant that all of the functionality be tested at the flight critical-level of certification. The trend for UAVs is to rely on time-space partitioning (e.g. ARINC 653) to effectively separate the two functionalities and assume non-interference. While this may work from a performance viewpoint, the failure mechanisms of the partitioning must be considered and understood when determining the probability of loss of control (PLOC) and fault tolerance of the system. As with other flight critical functionality, the failure mechanisms have to be validated then by testing. As the two criticalities are sharing resources, the impact of hardware failure must be predictable and testable. This means that the hardware architecture of the computation platform is a factor, which will drive up testing cost due to the countless variations



Mixed Critical Architecture Requirements



Mixed Initiative Challenge

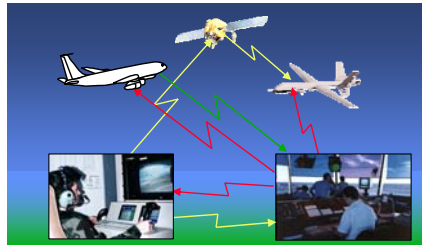


How can man and autonomy safely interact?

SOA: Human operator always get authority!

Issue:

Human operator may not have all the information or be able to comprehend situation in real-time:



- Situational Awareness versus Response Time
 - Assessment of UAV mode/state/health
 - Assessment of surrounding environment
- “Consequence of mishap” is a factor
- Complete system health is a factor
- Workload is a factor

Answer may reside in a authority management specification that would allow the correct party to have decision authority.

Mixed Initiative/Authority Management: As UAV systems become larger and more autonomous, the interaction with human operators becomes more complex. The implication of autonomy is that some of the decision-making responsibility resides with the vehicle, so the ability for humans to maintain adequate situational awareness may be reduced. A good example of this would be the interactions of the vehicle guidance, the ground operator, a collision avoidance function, and an air traffic controller. Each of these functions (human or otherwise) may have a different assessment of the situation and therefore, a different corrective action. One of the functions should have authority for corrective action. The decision for authority has to consider each function's: 1) situational/environmental awareness, 2) health, and 3) response time for corrective action. The test space for functional interaction is very large depending on the set of anticipated situations, the varying environmental factors, and health situations.



Mixed Critical Architecture Requirements



Multi-Entity Challenge



How can trust systems with multiple players to safely perform cooperative functions?

SOA: Keep humans away and hope for the best...

Issue:

Entities participating in the coordinated function may not be part of individual V&V testing:

- Linked Interface Control Documents?
- Entities with different manufacturers?
- System Configuration Management?
- Mission-specific programming?



Answer may reside in a specification for contingency management, based on system degradation

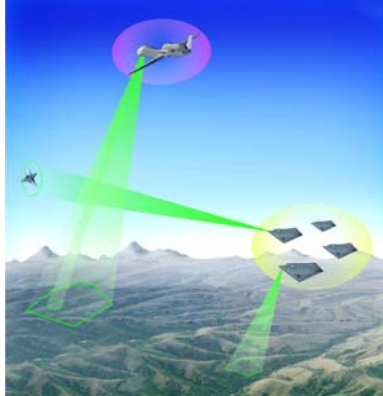
Multi-Entity: As systems become more autonomous, the natural trend is to develop functionality that calls for the cooperation between multiple entities. Examples of this are collision avoidance, cooperative control, and automated aerial refueling. The issues with multi-entity functionality stem from the fact that each entity will likely be certified separately and the whole function will never be truly tested since the different entities may be from different manufacturers. For development and testing, an interface specification will have to be used, but it will be highly complex in order to adequately describe the entity interactions during normal and degraded operation. For some multi-entity functions, the number of participating entities is variable and/or situational. This characteristic compounds the certification problem. Some of this functionality will require mission-specific programming while it is in operation, so it will need some form of quick certification to assure safe execution of the mission.



Mixed Critical Architecture Requirements



High Confidence Sensing Challenge



How can we trust visual/radar systems for flight critical functions?

SOA: Brute force and analytic redundancy

Issue:

Mission-style sensors don't have acceptable real-time methods for FDIR...

- Sensors will likely be multi-function!
- Redundant HW may not be answer, redundant information?
- Built-in-test may not provide good real-time coverage.
- Reliable signal processing/sensor fusion software

Answer may reside in sensor designs that compensate for sensor degradation and plan for contingencies

Sensor fusion: Historically, flight critical sensors have been very simple devices that produced discrete measurands that could be compared against redundant copies to provide data integrity. To augment situational awareness for autonomous UAVs, sensors that were typically used for mission sensing are being considered. Vision-based and radar-based sensors are very complex and expensive, so redundancy may not be feasible. The sensor health is currently the only indicator for potential failure of the sensor, but this may not be adequate for real-time detection and it leaves isolation and recovery as an open issues. Since this new information is now more complex, techniques for integrity need to be developed, so a flight critical function can determine whether the information is good or bad. It is anticipated that these sensors will be multi-functional, sharing its duty cycle between flight and mission functions, so will have the same issues as mention in the Mixed Criticality section above.



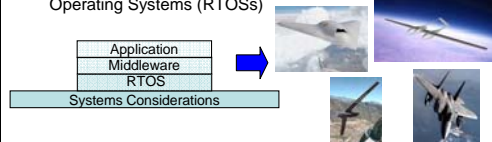
Mixed Critical Architecture Requirements

Boeing MCAR Project



Program Description

- Establish a new era of Flight Management Systems architecture definition and systems engineering
 - Incorporating a design-for-airworthiness certification philosophy
 - Considering Systems issues, Middleware, & Real-Time Operating Systems (RTOSs)



Technical Approach

- Requirements capture from current, emerging, and future Boeing platforms
 - Requirements refinement in collaborative Working Group meetings
- Requirements analysis with Architecture Tradeoff Analysis Method (ATAM)
- Requirements reasonableness checks and “art of the possible” inputs from the leading embedded flight software Middleware and RTOS vendors
- Folding in architectural insights and research results from NSF research teams



Technical Challenge

- Composability, including “Design for Certification” and use of “pre-certified components”
- Real-time performance
- Safety
- Develop requirements for systems, Middleware, and RTOS that are
 - Achievable Technically
 - Affordable
 - Have acceptable Risk
 - Adequately Meet Stakeholder Needs
- Some challenges to be posed to NSF research community



Program Information

- **Period of Performance:** 6/11/2007 to 6/5/2009
- **Program Plan:** Semi-Annual Working Group Collaborations and cycles of Requirements Capture & Analysis
- **Subcontractors:** Green Hills Software, LynuxWorks, Wind River Systems, Objective Interface Systems, Real-Time Innovations
- **Boeing Points of Contact:**
 - Dr. Jim Paunicka james.l.paunicka@boeing.com (Overall)
 - Dr. Doug Stuart douglas.a.stuart@boeing.com (M'ware)
 - Jim Barhorst jim.barhorst@boeing.com (RTOS)



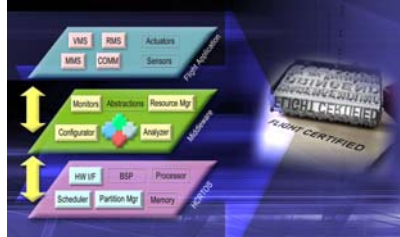


Mixed Critical Architecture Requirements

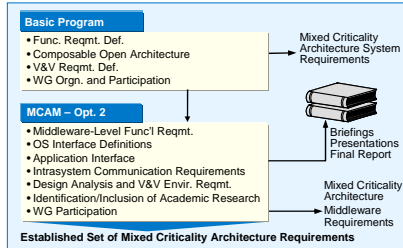
Northrop Grumman MCAR Project



Program Description



Technical Approach



Technical Challenges

- Defining Common/Consistent “certifiability” characteristics
- Defining functions To Implement characteristics (MW,RTOS)
- Defining Metrics to Assess characteristics and functions

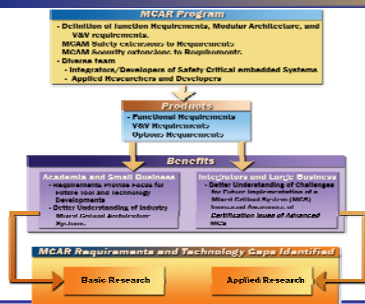
Program Information

- Program Status
 - Preliminary Framework Started
 - Initiated External Interaction with (3) Academic partners
 - Commenced Literature Review
- PI: Dr. Prakash Sarathy, (310) 332-0166
sriprakash.sarathy@ngc.com
- POC: Leonel Rico, (310) 505-2177
leonel.rico@ngc.com



Mixed Critical Architecture Requirements

LM Aero Team MCAR Project



Technical Approach

- Exploring the expansion of middleware to include services that are made of both safe and secure components. This new MCAM will become a modular/extendable framework for the blended/mixed environment of flight critical and mission critical systems of future UASs.

Technical Challenge

- How to isolate/blend the safety and security middleware services?
- What areas need to be addressed by academia? Robust partitioning of services beyond the current time and space partitions.
- What innovations are needed? New methods and tools for multi-core processor to expand middleware to support these, composable certification and support for multi-levels of scheduling to support mixed critical environment.

Program Information

- Current Status is that our team is working the initial characterization of middleware components/services for Safety and Security attributes of a mixed critical UAS.
- MCAR requirements phase and baseline architecture is Scheduled to be completed in Summer of 2009.
- POC: Peter Stanfill
Peter.O.Stanfill@lmco.com
(817) 935-1060



Mixed Critical Architecture Requirements Summary



- Many technical challenges associated with certification of intelligent and autonomous control systems
- Advanced UAS capabilities under development today will challenge certification (V&V) techniques far beyond their current capacities
- Lags in research for certification technologies will have a significant impact on levels of autonomous control
- Mixed-Criticality Architectures are needed Where SAFETY and SECURITY are Designed for Certification

There are many technical challenges associated with certification of intelligent and autonomous control systems. Advanced UAV capabilities being developed today will challenge certification techniques far beyond their current capacities. New V&V technologies are needed to enable timely and efficient certification of the intelligent and autonomous UAV control systems still in their infancy. V&V tools are needed to achieve the necessary degree of rigor that will ensure safety and security are designed simultaneously to mitigate risks associated with implementing autonomous control.