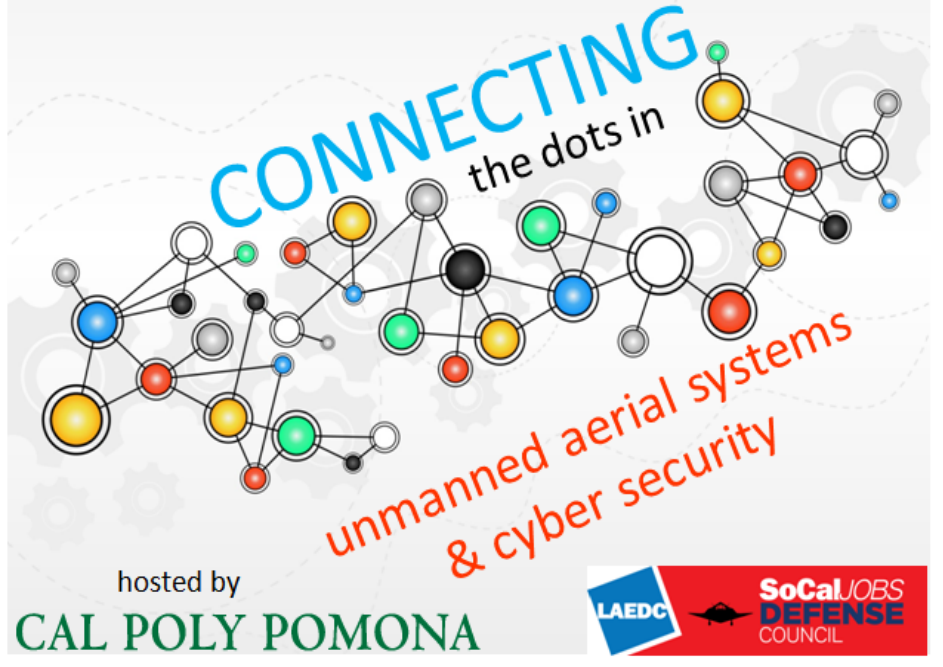


Panel 3
Future Direction: Increased Autonomy

December 12, 2014
Dr. John Vian, Technical Fellow
john.vian@boeing.com

The Boeing Company

Founded in 1916 in Puget Sound region of Washington state with a heritage that mirrors the history of flight. Aerospace pioneers now part of the Boeing enterprise include: North American Aviation, McDonnell Douglas, Rockwell International (space and defense business), Hughes Space & Communications, and Jeppesen.

Boeing Commercial Airplanes

Integrated Defense & Space Systems

Finding, creating, integrating and replicating technology solutions, processes, and leadership skills across the enterprise and the globe.

Engineering, Operations & Technology
Boeing Research & Technology

Boeing Central Research, Development and Innovation organization creating the future of aerospace

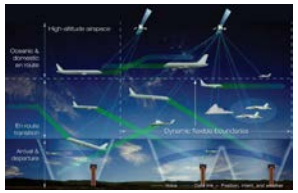
Autonomous Collaborative Systems-- The Opportunity

Cooperative automated systems can reduce the cost while also improving performance when compared to today's generally single-platform solutions-- whether it is in terms of goods moved, area searched, communication coverage, surveillance persistence, enemy suppressed, or environmental parameters monitored.

"complex/coupled systems"

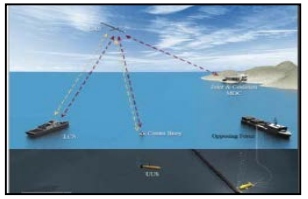
Large number of on/off-board sensors
Large number of interdependent decisions
Large number of failure modes

More-autonomous airplanes will interact intuitively and safely with future generation pilots and NextGen ground/space-based communication & control systems.



NextGen Commercial

Autonomous multi-aircraft systems will perform defense & security by operating in teams and swarms to execute complex missions with minimal human supervision.



Defense & Security

Air and ground vehicles will be on the internet-of-things performing search & rescue, environment monitoring, and agriculture services in teams with humans.

Civilian UAS

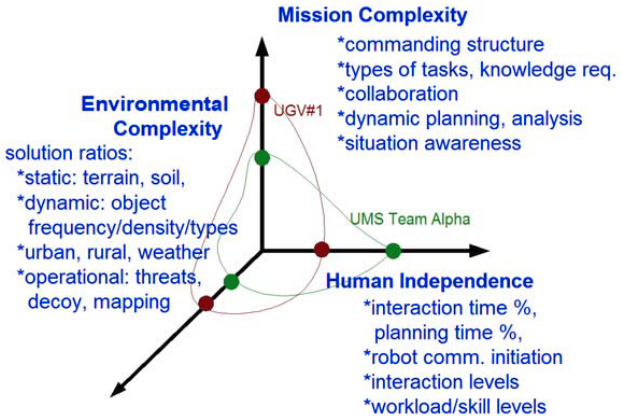
Heterogeneous mobile robot teams will autonomously perform complex assembly tasks without factory infrastructure.

Automated Assembly

Future aerospace systems will be more *autonomous* and *interact* with many other components (e.g. they are becoming ***complex/coupled systems***)

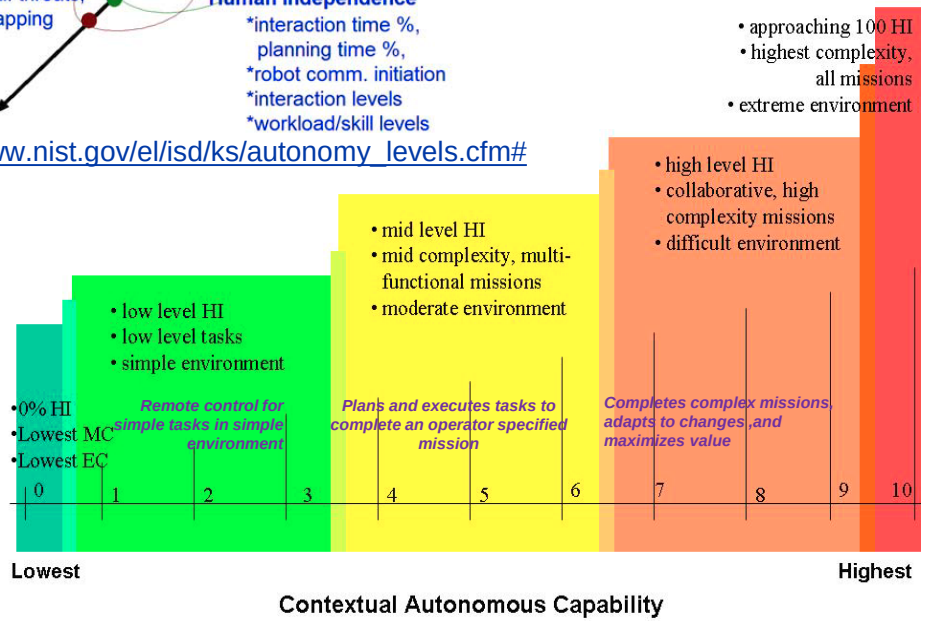
Autonomous Collaborative Systems-- The Challenges

Autonomous cooperative systems can reduce operational costs and improve performance. However, *control system design, verification, validation, and certification will be difficult.*



http://www.nist.gov/el/isd/ks/autonomy_levels.cfm#

Accommodating increasing system *complexity* is very difficult.



Automating *coupled* systems without degrading safety, mission assurance, and security is very difficult.

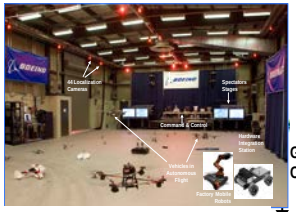
http://www.ntsb.gov/investigations

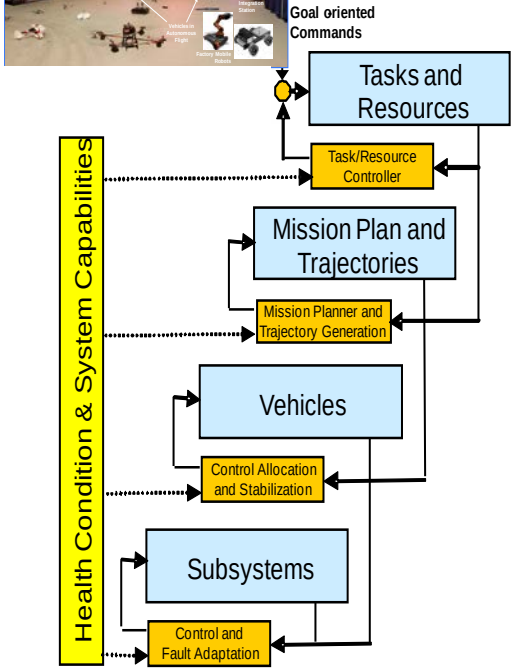
Examples from today's "simple" systems warn of challenges ahead...

Control system engineers, while dealing with difficult challenges to ensure safe and predicable performance, *must now also address cyber-physical system security*.

Hybrid Systems-- Health-adaptive Framework and Technology

A common basis of control systems technology can be applied across many multi-vehicle autonomous system domains. Cyber-physical systems security technology can be leveraged in the same manner.





Health-adaptive Architecture

Core Autonomy Technology

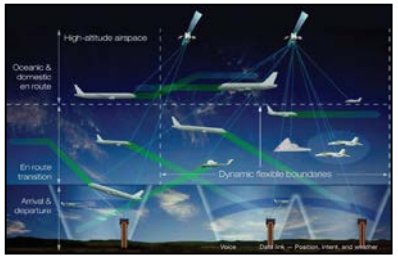
- **Automated tasking & sequencing**
- **Cooperative control algorithms**
- **Health-adaptive architectures**
- **Automated & adaptive mission management**
- **Automated asset assignment**
- **Multi-vehicle trajectory planning**
- **Automated de-confliction & collision avoidance**
- **Safety & emergency behaviors**
- **Automated fleet operations & sustainment actions**
- **Carefree human control and interaction**
- **V&V by design**
- **…**

technology reuse to reduce development time & cost

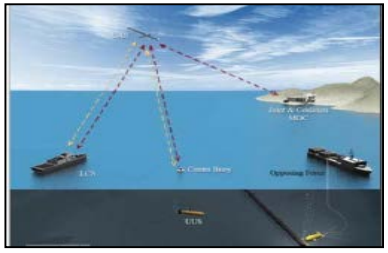
Applications

Factory Automated Assembly

Civilian UAS Applications



NextGen Commercial

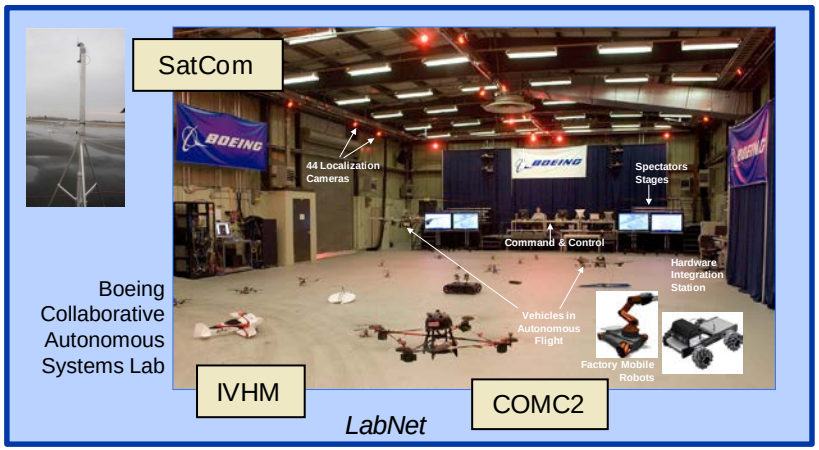


Defense UAS Applications

Health-Adaptive Autonomous Multi-vehicle Systems

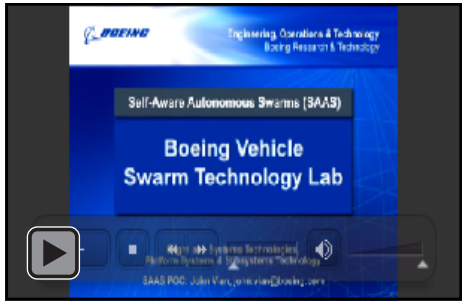
Cyber-Physical Systems Security Prototyping

Discover security issues earlier in the design phase by facilitating simultaneous analytic development and laboratory experimentation/prototyping using representative components.



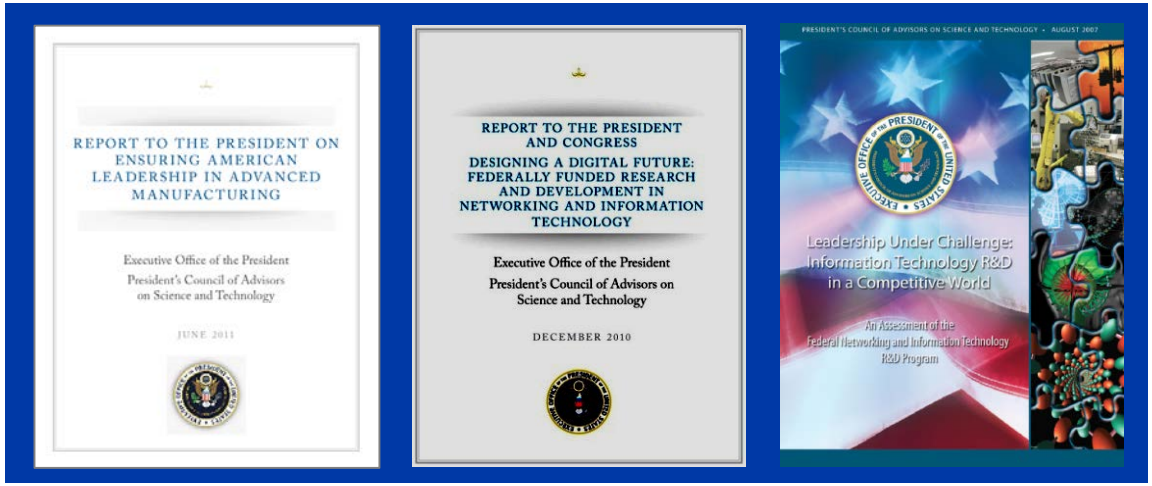
Experimental investigation of CPS security

- multi-core, memory arch, networking chips
- comm links, I/O, and component security
- safety, security, privacy, and workload
- computing and sw fault tolerance
- component damage/degradation tolerance
- mixed criticality function assessment
- tasking/scheduling run-time optimization
- upset recovery robustness
- security protocol verification
- environment modeling/accommodation
- hacker vulnerability / anti-tamper
- analytic and formal methods verification
- cross-domain reuse risk reduction
- other



Government/Industry/University Research Opportunities

Leadership in cyber-physical systems has become a national priority. Ensuring the security of these systems is vital to their acceptance.



University/Industry research endeavors in Cyber-resilient Unmanned Airborne Systems can leverage emerging opportunities from government agencies such as NASA, NIST, NSF, AFRL, AFOSR, ONR, FAA, DNR, NOAA, and others.

Questions, Feedback, and Comments