THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

MC2 Challenges for Mission Management of Unmanned Systems

An industry perspective

Second TCRTS Workshop on Certifiable Multicore Avionics and Automotive Systems (CMAAS)

Dr. Prakash Sarathy *(sriprakash.sarathy@ngc.com)*

Northrop Grumman Aerospace Systems

Space Park, Redondo Beach CA

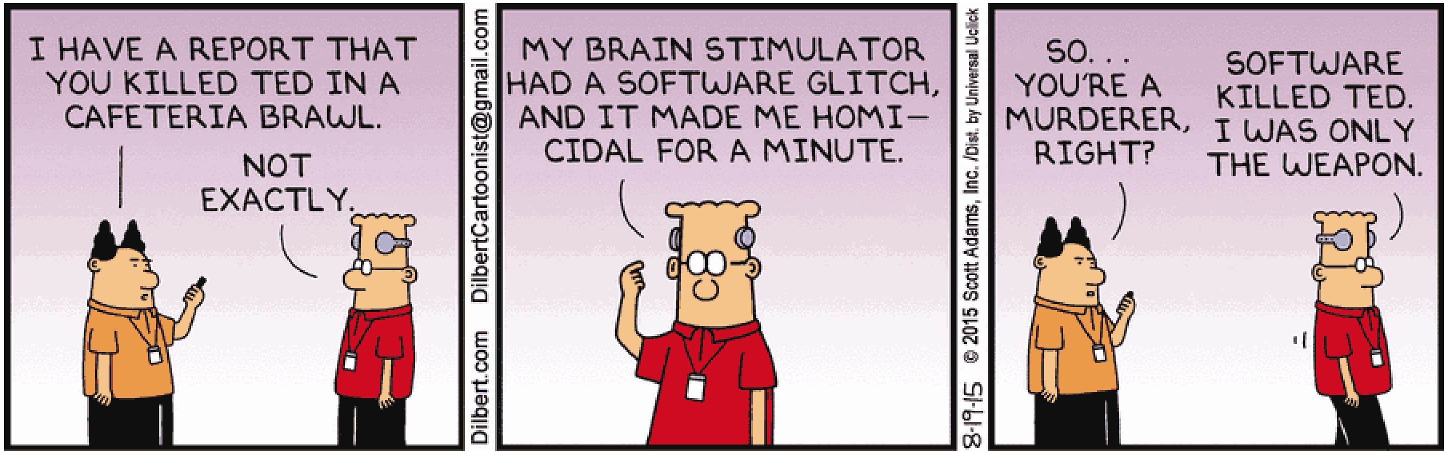
Motivation

NORTHROP GRUMMAN

- Enhancing and Ensuring Safety (Behavior Assurance)
- Ensuring Affordability
- Managing Complexity
- {Avionics} + {DecisionCapability} + {Sensing} + {Actuation} $\Rightarrow$ **CPS**

Increasing Mission Complexity

Goal: Provide insights into CPS drivers for unmanned systems


I HAVE A REPORT THAT YOU KILLED TED IN A CAFETERIA BRAWL.
NOT EXACTLY.
MY BRAIN STIMULATOR HAD A SOFTWARE GLITCH, AND IT MADE ME HOMI-CIDAL FOR A MINUTE.
SO. . . YOU'RE A MURDERER, RIGHT?
SOFTWARE KILLED TED. I WAS ONLY THE WEAPON.
Dilbert.com DilbertCartoonist@gmail.com
8-19-15 © 2015 Scott Adams, Inc. /Dist. by Universal Uclick

Autonomous Operations Challenges

NORTHROP GRUMMAN

- Autonomy Spectrum
  - "A thrown stone is a perfectly autonomous system" (zero control response)
  - Manned fighter is also an autonomous system (lots of intelligent control!)
- Autonomy
  - is not a useful scale! (Flawed by definition), but is a vital system trait for UxVs
  - Better to think of autonomous operations in terms of req.s and design functions
  - Not inherently unsafe, just harder to understand and determine outcome
- Key Challenges
  - Mixed Initiative Transparency and Communications (Trust, Explanations)
  - Self-Assessment and Reflection (Oracles/Monitors)
  - Bounded Functional Characterization (?)

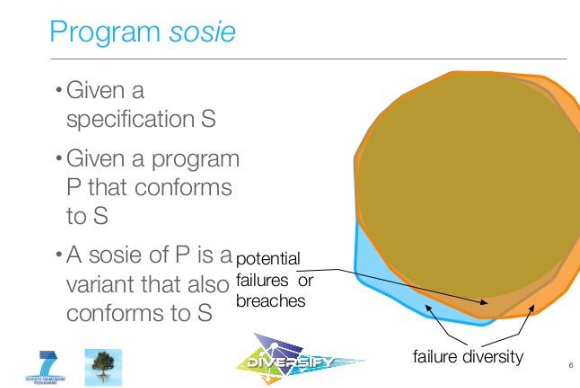
Frozen Double Shot Macchiato Skinny with no Ice…

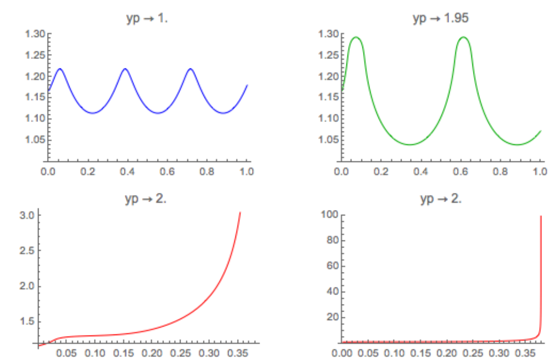
Approved for Public Release: NG16-1434, 7/25/16

Role of Resiliency in Autonomous Operations

NORTHROP GRUMMAN

- Flexibility / Rigidity
- Stiff Systems
- Diversity
- Originality /Creativity





Resiliency Essential to be Mission Effective under off-nominal conditions

Approved for Public Release: NG16-1434, 7/25/16

Mission Drivers

NORTHROP GRUMMAN

- Dynamic
  - Tasking changes throughout mission
  - Actors (Blue/Red) change as well
  - Environment is dynamic in that both the operating conditions and the relevant situation are continually subject to change.
- Uncertain
  - Integrity of sensed data is often very limited
  - Expectations of operating conditions is limited to short timescales
  - Blue and Red Actor (human) responses exhibit a high degree of uncertainty
- Adverse
  - In Theater operations have to contend with an active adversary
  - Some basic strategy and tactics will need to be modeled and extant as part of the unmanned system

Challenges of complex missions drive CPS capability set

Avionics Constraints

NORTHROP GRUMMAN

- Embedded Processing is limited by SWAP and Flight qualification
  - Small number of embedded boards available that are flight qualified
  - Significant limitation on available processing power due to SWAP constraints
  - Additional constraints placed for special operating conditions such as Carrier (CV) Suitability (E3, Shock and Vibration)
- Architecture
  - Avionics Architecture subject to Interoperability standards such as FACE
  - Architecture is constrained by its integration (usually tight coupling) with other safety critical components (flight controls, navigation, stores)
  - This impacts memory, available data bus, physical interfaces
- Integration
  - Vertical integration often drives the form and function of the avionics processing trade space

Reliability and SWAP drive onboard processing requirements

Safety Challenges for UxV: 1…2…3…

1. Why is this hard?
   - Consensus on the right _safe_ behavior
   - No integrated tools/framework to establish assurance
   - Doing more -> More Autonomy -> More complexity

2. Why is this costly?
   - Current verification relies primarily on exhaustive testing ($$$)
   - Software complexity (combinatorial) $\propto$ Testing cost ($$$$)
   - Input Space $\otimes$ Decision Space $\otimes$ Output Space $\Rightarrow$ Infeasible Test Size

3. Why is this so murky?
   - No objective / functional framework for Safety Characterization
   - "Do no wrong" - Prove that UAV will avoid situations in which it cannot cope with or handle
   - Regulatory Uncertainty further complicates these issues

Safety is hard, but should you care?

Safety Drivers: Lifecycle Approach

NORTHROP GRUMMAN

- What's out there?
  - Requirements Specification/Analysis/Validation Tools
  - Formal Methods: Model Checking, Reachability sets, syntactic parsing, automated case generation …
  - Design for safety: Composability contracts, stability/safety bounds, oracles, safety controllers, monitors …
  - Safety guidance for implementation (MILSTD882/JSSSEH/AOP52…), Simplex Architectures (multicore), adaptive scheduling
  - Verification Tool chains: coverage tools,

- What do we need?
  - Requirements/Arguments/Formalism
  - Design for safety certification guidance, models, sw constructs
  - Build/Implementation guidelines
  - Test/Verifications process, evidence collection
  - Making the certification case/licensure

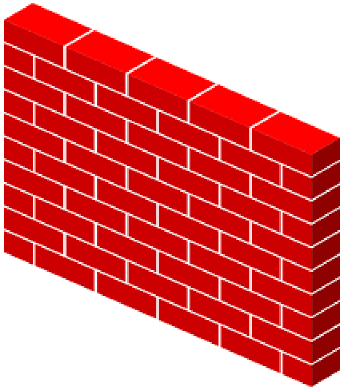
A holistic approach to Safety demands resiliency

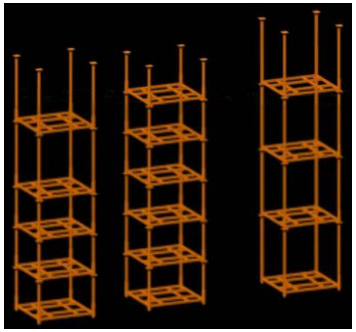
Approved for Public Release: NG16-1434, 7/25/16

Security Drivers

NORTHROP GRUMMAN

- Time and Space Partitioning (SWAP, Architecture)
- Multiple Enclaves (SWAP, Data availability)
- Virtualization/Partitions (Data movement constraints)
- Security Principal / Kernel (Latency, data movement)





Can't Live without it, Cannot live with it …

Affordability & Interoperability Desirements

NORTHROP GRUMMAN

- Interoperability Standards
  - FACE, UCI, STANAG 4586, JAUS, IOPs
  - Cross-Domain Standards
  - Open Architecture – OASIS, RedHawk
  - Generalization of Data Models
- Affordability
  - Product Line approach + SOA
  - Common/Core Components + Variants/Custom Components
  - Open Business Model

Interoperability is desirable but hard to achieve for unmanned CPS

Unmanned Edge Cases of current relevance

NORTHROP GRUMMAN

- Case 1: Loss of Communications
  - Latency, Bandwidth/Throughput, Reliability, Loss, Adverse Action
  - Knowing (detect/perceive), Planning(problem-solving), Doing(fuzzy-execution)
- Case 2: Subsystem Failure
  - Prognostics, Diagnostics, Detection, Isolation
  - Respond/Rework, Switch/Swap/Substitute, Change/Alter, Assess Impact
- Case 3: Cooperative Operations
  - Mission Lifecycle – SA, Plan, Act = Teaming?
  - Planned / Unplanned ?
  - Good Samaritan vs. Greedy Approaches

Run-of-the-mill ? Real Challenge for Unsupervised Operations

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

Putting it together

Building a case for UxV Certification

NORTHROP GRUMMAN

- Tesla, Ravens, Quadbots, Remus, iRobots : UxVs coming home to roost…
- UxV proliferation is a real problem – in the air, underwater and on the ground
- Potential issues include controlled space conflicts, loss of control, loss of privacy, parking conflicts
- Potential hazards range from UxV pile-ups, property incursions, package rain, falling debris…
- Resilient and Self-Aware systems can greatly accelerate development of Safe Behavior Bounds for CPS systems, but pose real challenges for Schedulability

"UxV's" are very real and now in a neighborhood near you!

Implications for Schedulability and Scheduling

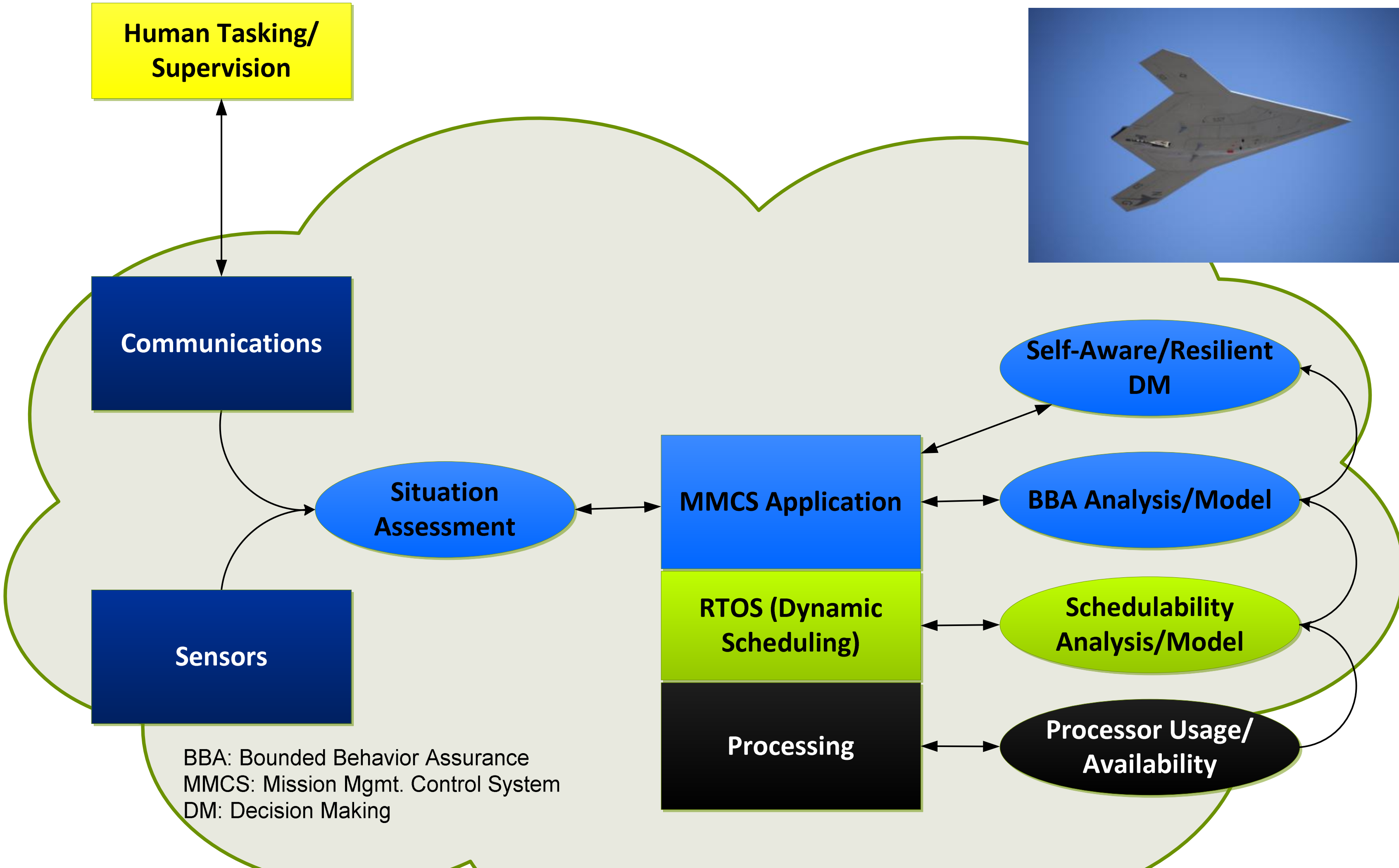
NORTHROP GRUMMAN

Desired Capability		Impact
• Respond to Dynamic Environment	→	• Unpredictable events trigger bounded set of behaviors
• Dynamic Decision Making	→	• Any selected behavior response can/will change over its implementation
• Enhanced Situation Awareness	→	• SA can give a heads up on impending changes
• Resilient Response to adversity	→	• In a degraded system solution, decision making should include an assessment of schedulability

Challenges inherent in unmanned CPS are multi-disciplinary and cross-layer

In a future CMAAS …

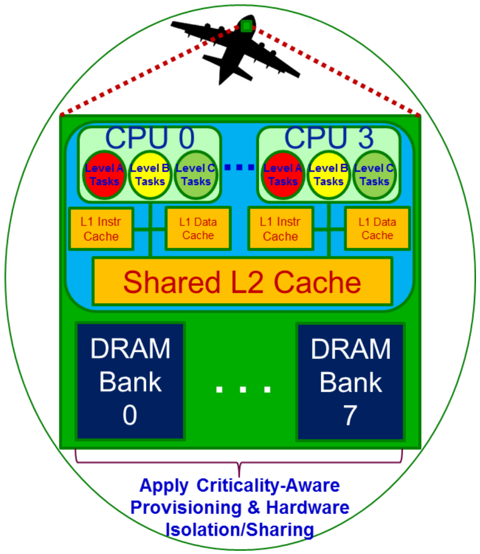
NORTHROP GRUMMAN



Realizing Assured Mission Management Avionics will need your help!

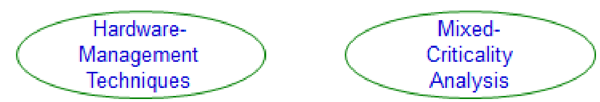
NGC Collaboration with Jim Anderson UNC

NORTHROP GRUMMAN



Our Solution Strategy

- W.r.t. lessening capacity loss generally (even on uniprocessors), two orthogonal approaches have been investigated previously:
  - » **Hardware-management techniques** that reduce hardware interference.
  - » **Mixed-criticality analysis techniques** that enable less critical tasks to be provisioned less pessimistically.

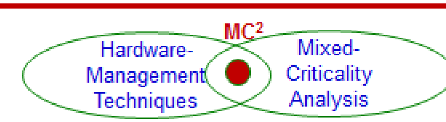


Future Work

- Our future plans include:
  - » Investigating other forms of IPC such as pipes and message queues.
  - » Conducting a definitive schedulability study that fully considers all options and allocation choices.
  - » Extending page coloring to fully deal with dynamically allocated pages.
  - » Enabling dynamic task-system adaptations, mode-change protocols, and synchronization.

Our Solution Strategy

- Our work focuses broadly on research questions that arise when applying both approaches together.
  - » We are addressing such questions in the context of a resource-allocation and analysis framework developed by us called **MC² (mixed criticality on multicore).**



Note: All material in this slide reproduced by permission from Jim Anderson UNC

Path Forward

- A broad spectrum of needs and drivers for unmanned CPS have been discussed
- The challenges posed need a comprehensive approach, both functional and non-functional, to make inroads
- A foundational construct that can have wide ramification is to la prior and online schedulability models to inform dynamic responses to external events
- Such a multi-level resilient system when informed by schedulability and implemented by advanced scheduling approaches, can produce assured desirable behavior under dynamic, uncertain and adverse conditions

Thank You

THE VALUE OF PERFORMANCE.