



Humans and Robots Working Together Safely

Space Exploration Conference

Randy Black

December 6, 2006

Audience Response: Primal Fears in the Information Age



Which out-of-control autonomous system is the most dangerous?

- Colossus the Forbin Project
- HAL 9000 from 2001, a Space Odyssey
- WOPR from Wargames
- SkyNet from the Terminator movies
- The Gunfighter from Westworld

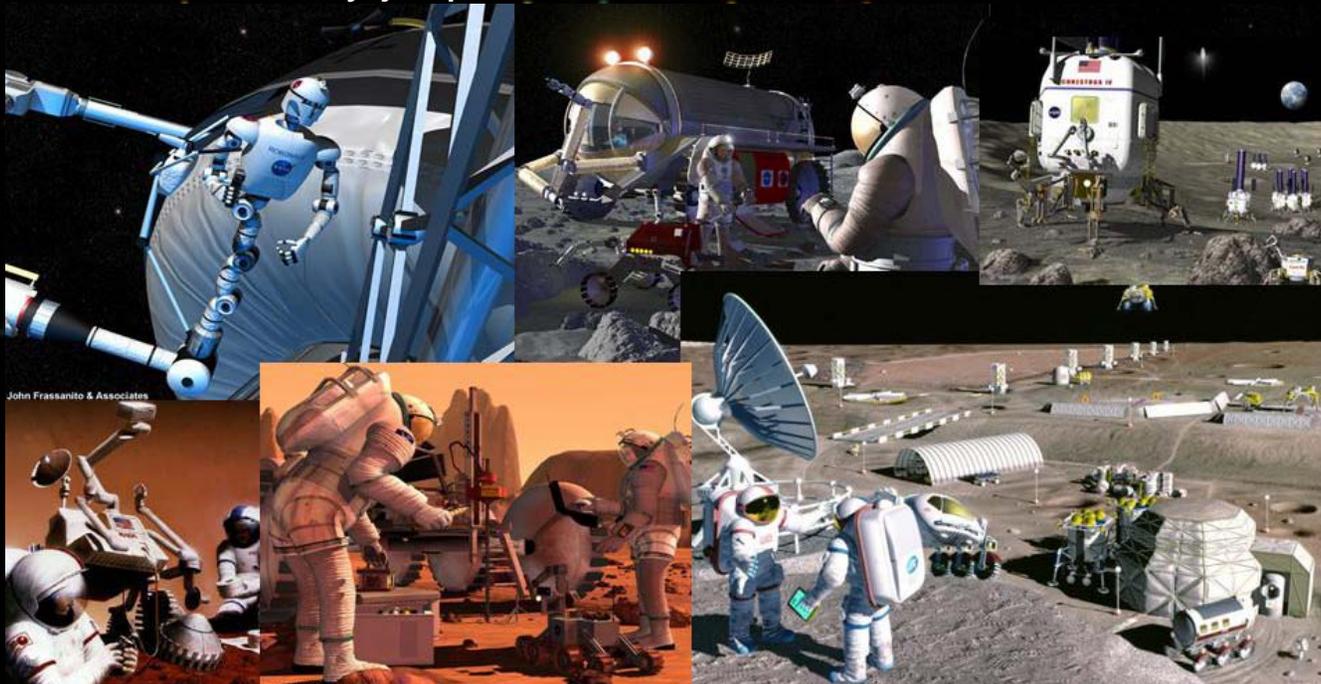
Dr. Doug Blank at Bryn Mawr University teaches a computer science seminar: Robots Gone Berserk

Implementing the Vision

The Problem



- Space exploration envisions numerous unmanned systems
- Unmanned systems require excessive human control
- Decreasing human control implies increased autonomy
- Increased autonomy implies decreased safety
- Decreased safety jeopardizes human life and mission success



Implementing the Vision

Hope: Asimov's 1st Law of Robotics

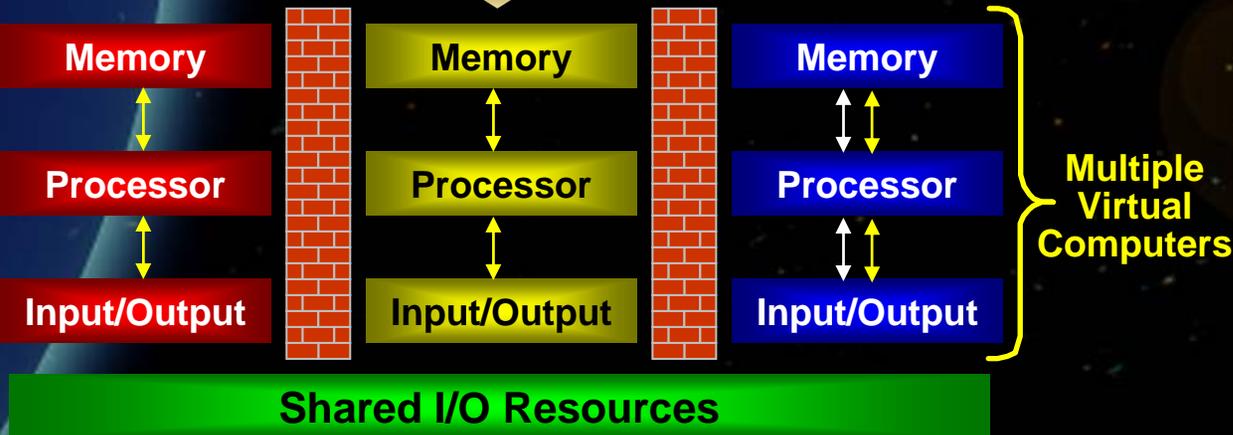
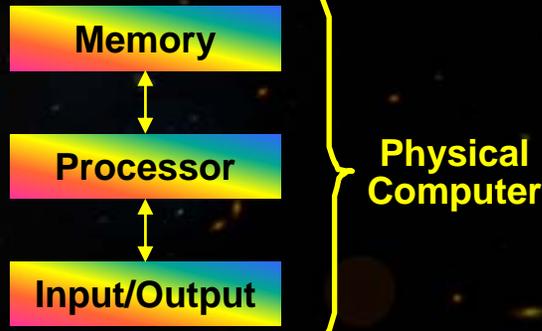


- A robot may not injure a human being or, ~~through inaction, allow a human being to come to harm.~~
- Archetype: Robby the Robot from Forbidden Planet
 - Chauffeur, Manual Laborer, Chef, Assistant, Chemical Analyst, Security Provider
 - Failsafe prevents harm to humans
- Could a similar failsafe be built into the controls of autonomous systems?
- Honeywell has been working to apply commercial Integrated Modular Avionics principles to autonomous systems controls
 - Same underlying principles support the Orion capsule avionics
 - Successfully flown over 40 million hours on commercial aircraft



Credit: Hammacher Schlemmer

The Technology: Robust Partitioning



Partitioning Domains

1. Memory Space
2. Computation Time
3. Input/Output Access
4. Backplane Access

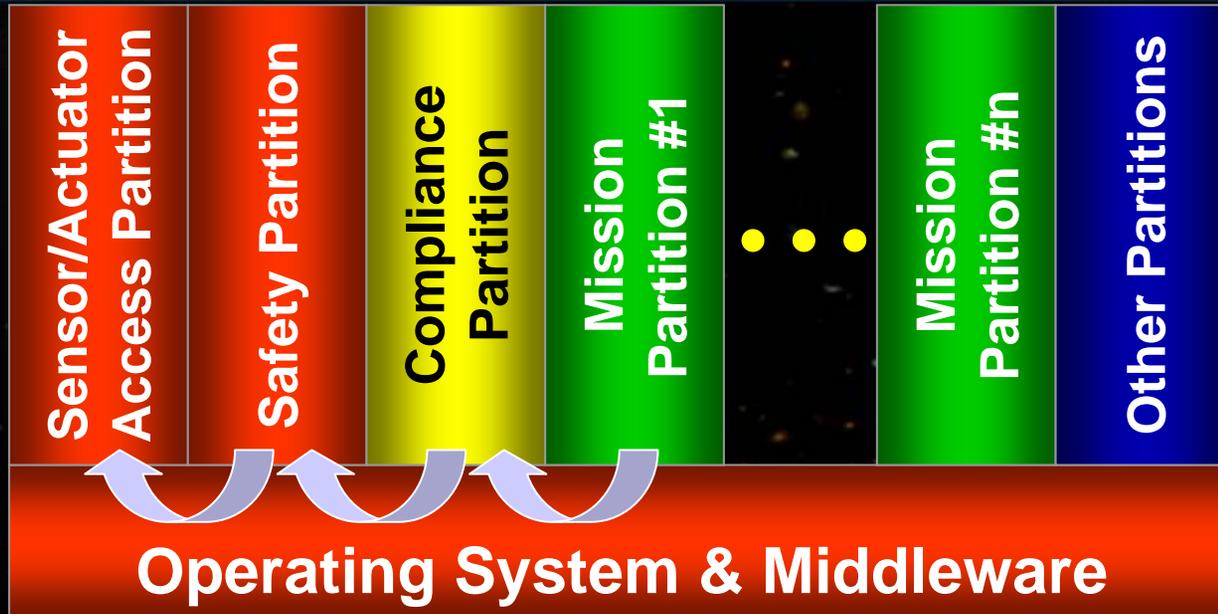
Technical Principles

- Hardware Enhanced Partitioned OS (ARINC-653)
- Table Driven Coordination of Processing Control and Data Movement
- Memory Mapped Interfaces
- Fail Passive Fault Response

Partitions form solid fault containment zones

Implementing the Vision

The Failsafe: A Safety Partition



- Iron clad partitioning allows safety overrides to non-deterministic autonomous algorithms
- Commands generated by applications must pass through a Safety Partition (at a minimum) prior to performing any actuation
- Safety Partition assures commands do not jeopardize human life or mission success
- The Safety Partition can be certified to a higher rating than the autonomous application software

Sample Safety Detection Scheme - UWB



- Ultra WideBand (UWB) employs a short pulse occupying 500 MHz or greater of the spectrum at low power, avoiding multipath anomalies
- No RF interference with on-board GPS, video, audio, and telemetry systems
- The UWB Systems Group at JSC has developed schemes for providing high data rate communication (supporting voice, video, telemetry, etc.), long range tracking (<1% error up to 3500 ft), and sub-inch position tracking at near range
- By placing RFID tags on the astronaut (or on equipment), UWB devices can compare the position of the astronaut with the path of the autonomous device and limit the force or stop the device if an unsafe situation occurs



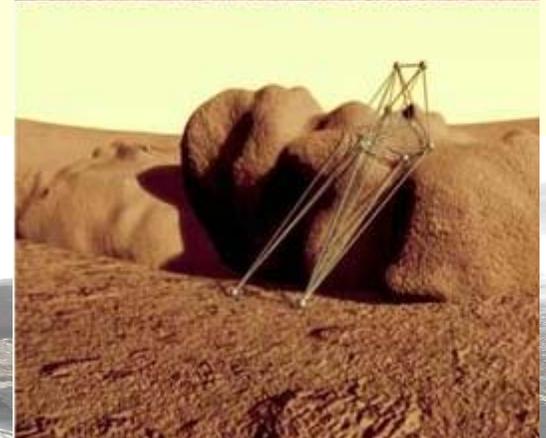
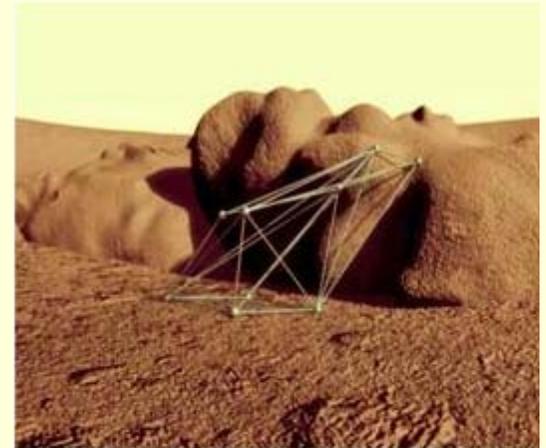
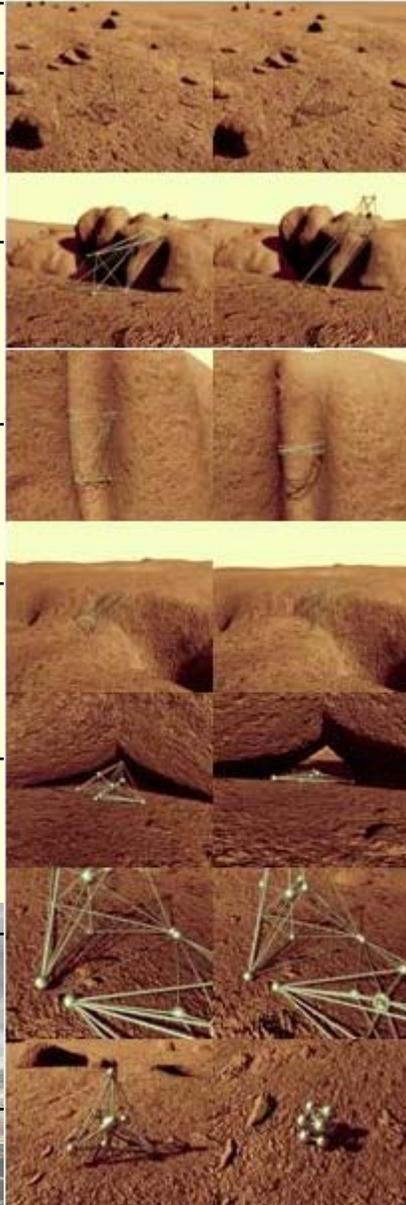
TET: High Mobility where Form follows Function



Example

Partitioned control can ensure the safety of the neural net decision making algorithms on the GSFC TET autonomous system

Terrain	Operation
Smooth, Low Relief	Roll
Rugged, Low Relief	Climb over obstacles
Cliff	Chimney up
Crevasse	Bridge
Opening	Flatten
Repair	Strut Exchange
Stow/Grow	Change Size



Conclusions



- Space Exploration envisions several unmanned systems operating simultaneously
- Cost constraints limit the number of operators available to interact with these unmanned systems
- Decreasing human interaction requires increased autonomy
- Increasing autonomy normally decreases reliability
- The technology exists to provide a reliable failsafe for autonomous systems
- This Safety Partition scheme can be used across a wide variety of applications, from autonomous rendezvous and docking to explorer robots