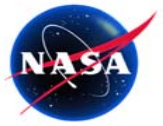


Honeywell

High Performance, Environmentally-Adaptive Fault-Tolerant Computing

9th High Performance Embedded Computing Workshop
@ M.I.T. Lincoln Laboratory

September 22, 2005

Dr. John R. Samson, Jr. - Honeywell Space System Clearwater, Florida
Jeremy Ramos - Honeywell Space System Clearwater, Florida
Dr. Alan George, University of Florida, Gainesville, Florida
Dr. Minesh Patel – Tandel Systems LLC, Clearwater, Florida
Raphael Some – Jet Propulsion Laboratory, California Institute of Technology

Contact: John Samson
Telephone (727) 539-2449
john.r.samson@honeywell.com

UNIVERSITY OF FLORIDA

Outline

Honeywell

- **Introduction**
  - New Millennium Program
  - Space Technology (ST) – 8 Project
  - ST-8 Project Schedule
  - EAFTC Technology Advance
  - Technology Validation Plan
- **EAFTC Flight Experiment**
- **EAFTC TRL 5 HW Baseline**
- **EAFTC TRL 5 SW Baseline**
- **Current Status & Plans**
- **Summary & Conclusion**
- **References**

UNIVERSITY OF FLORIDA

New Millennium Program (NMP) – Mission Statement

Honeywell

While an emerging technology may seem promising and likely to provide the technical capabilities NASA requires, it may also present an unacceptable risk to any exploration mission using it for the first time in space. The goal of NMP is to reduce the risks to, as well as the costs of, future NASA space science missions.

To meet it goals, the NMP identifies and selects leading-edge technologies that will increase the capability of future Science Mission Directorate missions. To identify the crucial technologies required, technologists are guided by the roadmaps of NASA's three mission areas: Sun-Earth System, Solar System, and Universe. The technical requirements outlined in these roadmaps are matched with technologies emerging from the national "pipeline" of current technology-development efforts. Once selected, these untried technologies are demonstrated on NMP in-space validation missions.

UNIVERSITY OF FLORIDA

ST-8 Mission

Top Level Requirements:

- Demonstrate and validate four (4) ST-8 technology advances in a relevant space environment
  - Environmentally Adaptive Fault-Tolerant Computing (EAFTC) experiment *
  - Miniature Loop Heat Pipe (MLHP) experiment
  - Next Generation Ultraflex (NGU) experiment
  - SAILMAST experiment
- Operate in space for at least 6 months

* Relevant space environment for EAFTC experiment is defined as a stressing application executing in the worst radiation environment expected for early adopter missions

New Millennium Program (NMP) – ST-8 Schedule (1)

Honeywell

JPL

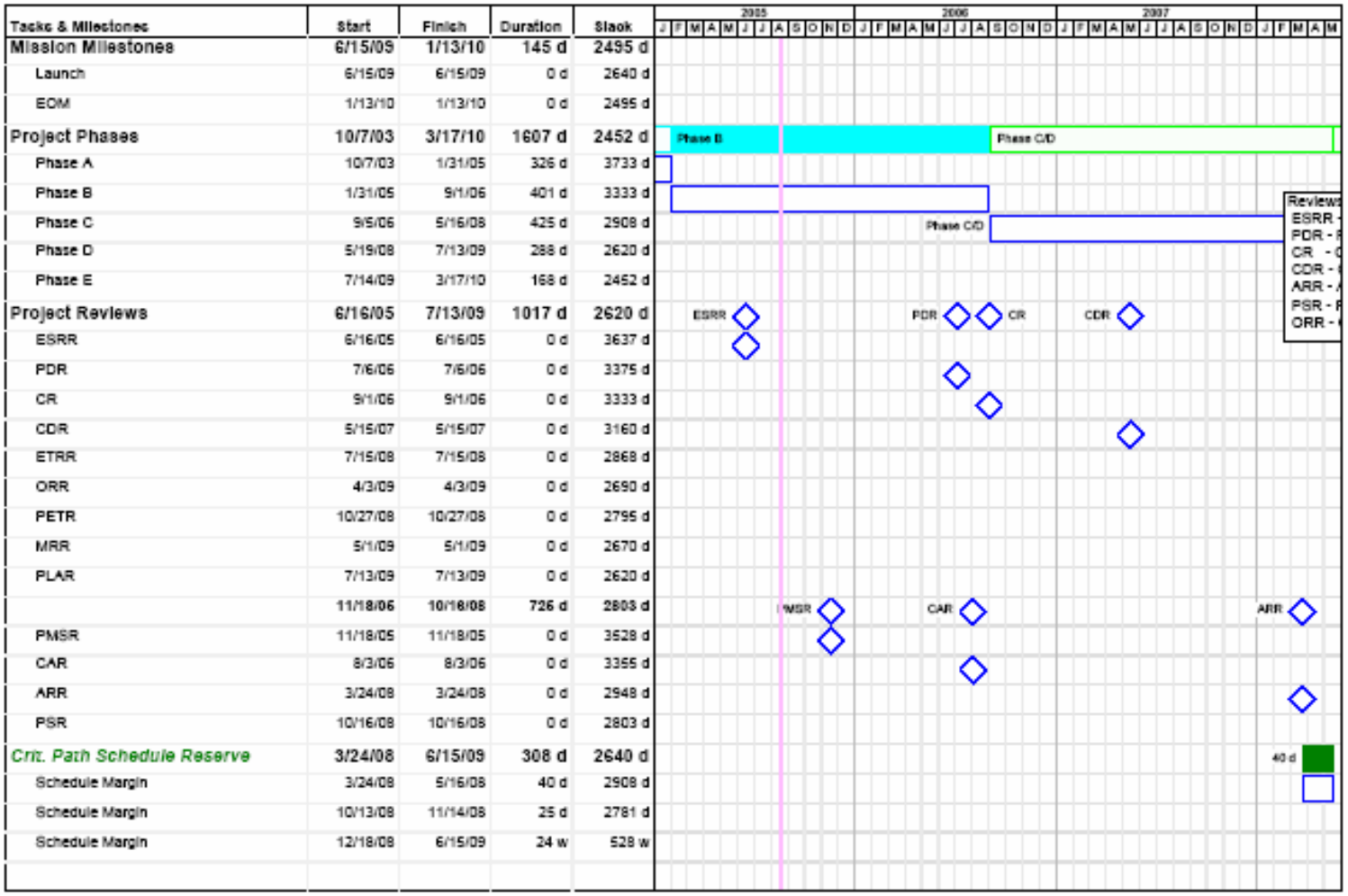
Responsibility: M. Bothwell
Revision Date: 8/17/05 8:43 AM

Preliminary Master Schedule

NMP-ST8

Project Schedule Analyst: Ryan H Montgomery
http://sched-central.jpl.nasa.gov/

Tasks & Milestones	Start	Finish	Duration	Slack
Mission Milestones	6/15/09	1/13/10	145 d	2495 d
Launch	6/15/09	6/15/09	0 d	2640 d
EOM	1/13/10	1/13/10	0 d	2495 d
Project Phases	10/7/03	3/17/10	1607 d	2452 d
Phase A	10/7/03	1/31/05	326 d	3733 d
Phase B	1/31/05	9/1/06	401 d	3333 d
Phase C	9/5/06	5/16/08	425 d	2908 d
Phase D	5/19/08	7/13/09	288 d	2620 d
Phase E	7/14/09	3/17/10	168 d	2452 d
Project Reviews	6/16/05	7/13/09	1017 d	2620 d
ESRR	6/16/05	6/16/05	0 d	3637 d
PDR	7/6/06	7/6/06	0 d	3375 d
CR	9/1/06	9/1/06	0 d	3333 d
CDR	5/15/07	5/15/07	0 d	3160 d
ETRR	7/15/08	7/15/08	0 d	2868 d
ORR	4/3/09	4/3/09	0 d	2690 d
PETR	10/27/08	10/27/08	0 d	2795 d
MRR	5/1/09	5/1/09	0 d	2670 d
PLAR	7/13/09	7/13/09	0 d	2620 d
	11/18/06	10/16/08	726 d	2803 d
PMSR	11/18/05	11/18/05	0 d	3528 d
CAR	8/3/06	8/3/06	0 d	3355 d
ARR	3/24/08	3/24/08	0 d	2948 d
PSR	10/16/08	10/16/08	0 d	2803 d
Crit. Path Schedule Reserve	3/24/08	6/15/09	308 d	2640 d
Schedule Margin	3/24/08	5/16/08	40 d	2908 d
Schedule Margin	10/13/08	11/14/08	25 d	2781 d
Schedule Margin	12/18/08	6/15/09	24 w	528 w



UNIVERSITY OF FLORIDA

New Millennium Program (NMP) – ST-8 Schedule (2)

Honeywell

JPL

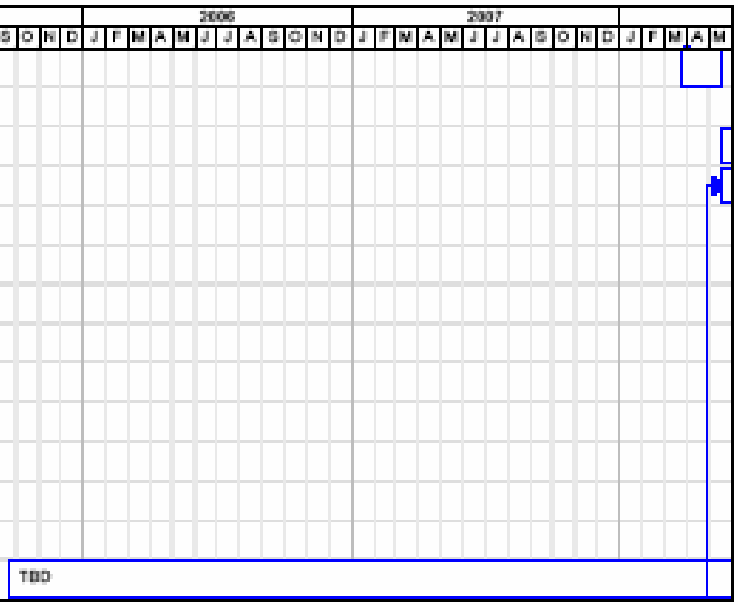
Responsibility: M. Bothwell
Revision Date: 8/17/05 8:43 AM

Preliminary Master Schedule

NMP-ST8

Project Schedule Analyst: Ryan H Montgomery
http://sched-central.jpl.nasa.gov/

Tasks & Milestones	Start	Finish	Duration	Slack
Reserve	3/24/08	5/16/08	8 w	581.6 w
Flight System ATLO	6/18/08	8/16/09	289 d	2639 d
S/C-Payload I&T	5/19/08	11/12/08	125 d	2639 d
S/C-Instrument I&T	5/19/08	6/16/08	1 mo	131.95 mo
System Performance Test	6/17/08	10/9/08	16 w	527.8 w
System TV Test	8/18/08	9/8/08	3 w	566 w
Reserve	10/9/08	11/12/08	5 w	527.8 w
Ship to VAFB	11/13/08	11/14/08	2 d	2639 d
Launch I&T	11/17/08	6/12/09	141 d	2639 d
Launch I&T	11/17/08	12/17/08	4.2 w	527.8 w
Reserve	12/18/08	6/12/09	24 w	527.8 w
Launch	6/15/09	6/15/09	1 d	2639 d
Mission Ops & Tech Validation	1/28/08	7/27/09	126 d	2810 d
Ground System Implementation	9/23/06	12/28/09	816 d	2764 d



UNIVERSITY OF FLORIDA

Processing Platforms for New Science

Honeywell

- The success of recent rover missions are a perfect example of the type of science we want to support
- Though returns from rover missions are significant they could be orders of magnitude greater with sufficient autonomy and on-board processing capabilities

- Similarly, deep space probes as well as Earth orbiting instruments can benefit from increases in on-board processing capabilities
- In all cases increases in science data returns are dependant on the spacecraft's processing platform capabilities

UNIVERSITY OF FLORIDA

EAFTC Experiment Overview - Technology Advance

Honeywell

- **A spacecraft onboard payload data processing system architecture, including a software framework and set of fault tolerance techniques, which provides:**

A. **An architecture and methodology that enables COTS based, high performance, scalable, multi-computer systems, incorporating reconfigurable co-processors, and supporting parallel/distributed processing for science codes, that accommodates future COTS parts/standards through upgrades.**

B. **An application software development and runtime environment that is familiar to science application developers, and facilitates porting of applications from the laboratory to the spacecraft payload data processor.**

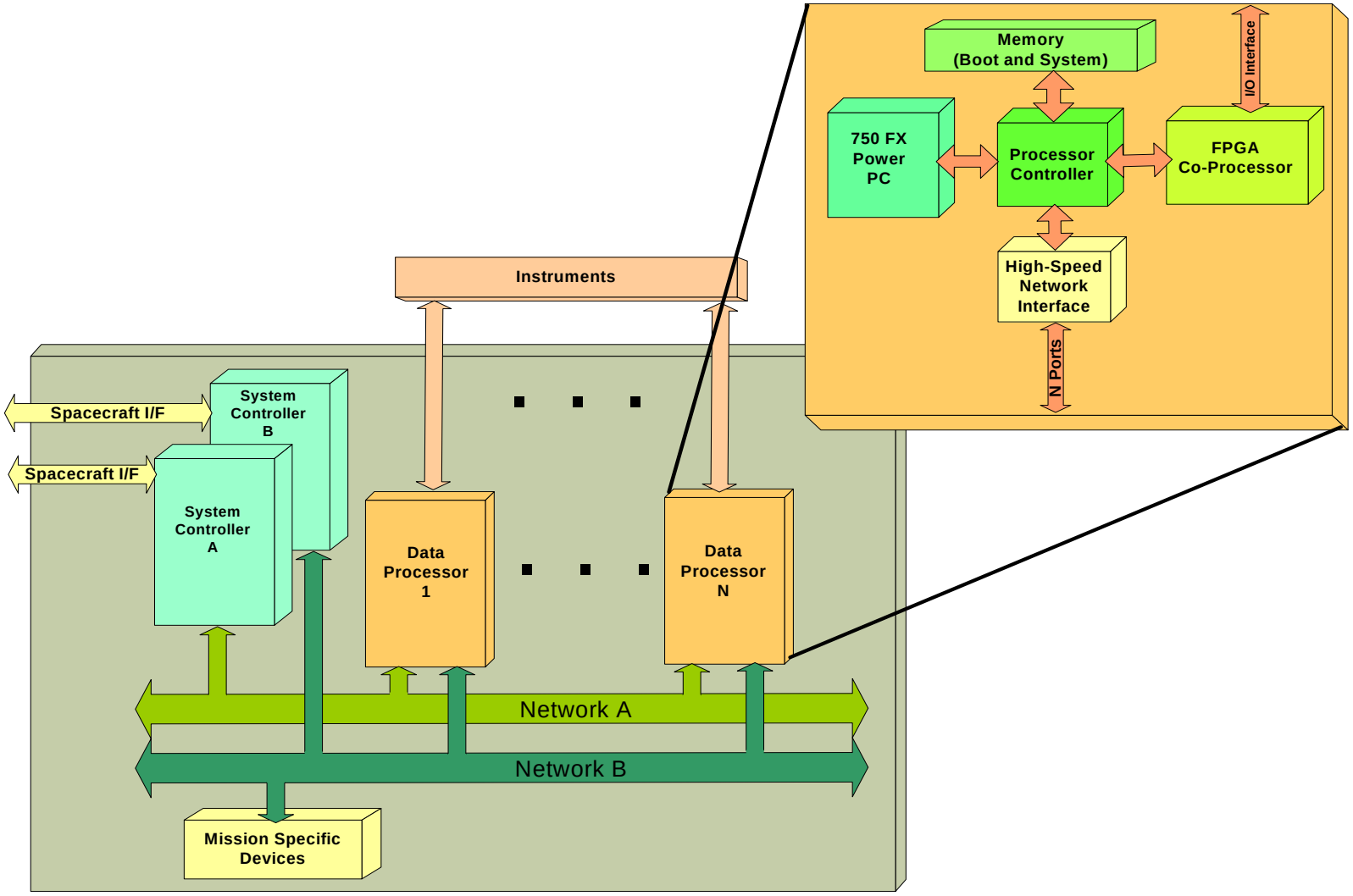
C. **An autonomous and adaptive controller for fault tolerance configuration, responsive to environment, application criticality and system mode, that maintains required dependability and availability while optimizing resource utilization and system efficiency.**

D. **Methods and tools which allow the prediction of the system's behavior in the space environment, including: predictions of availability, dependability, fault rates/types, and system level performance.**

UNIVERSITY OF FLORIDA

EAFTC Hardware Architecture

Honeywell

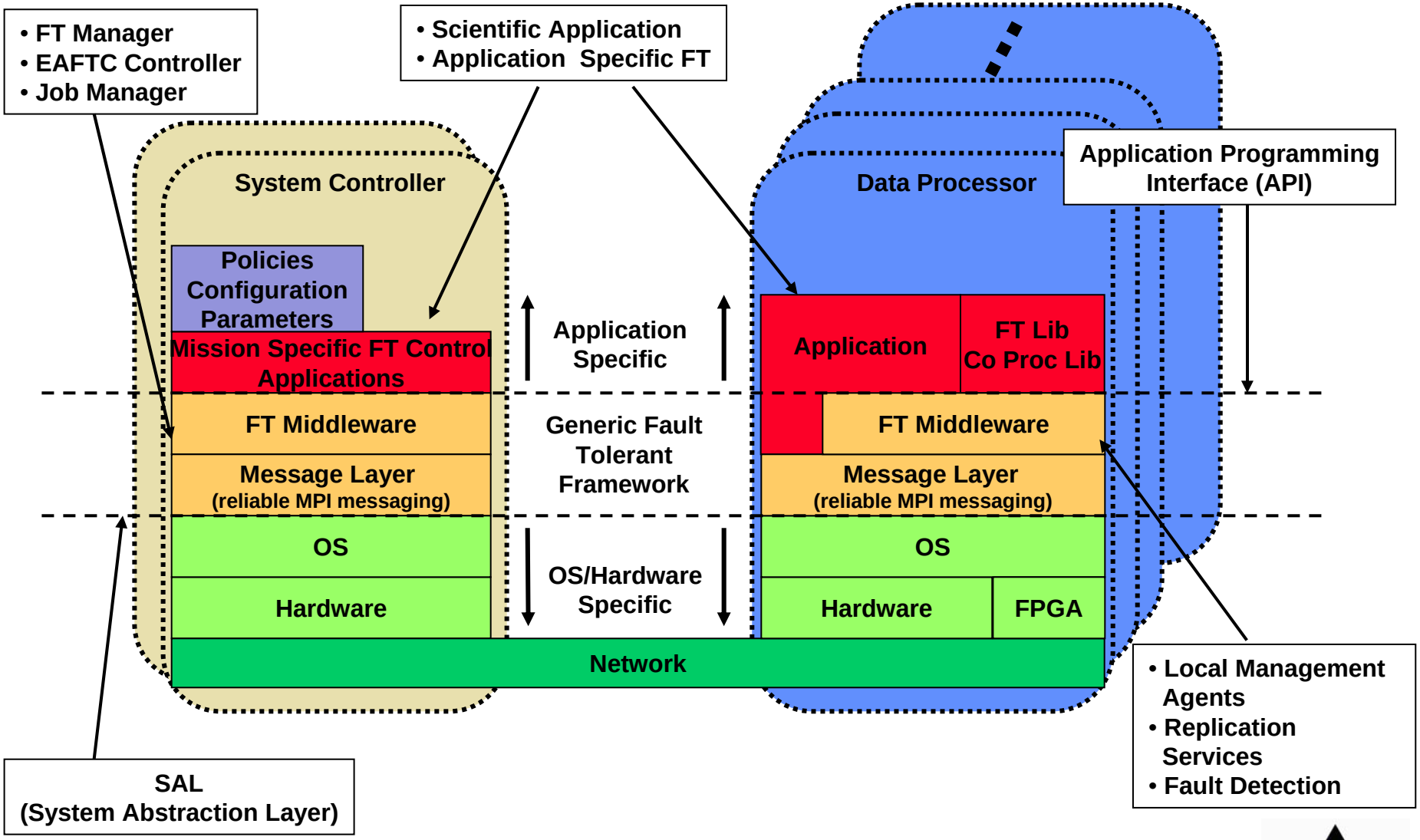


Addresses Technology Advance components A, B, and C

UNIVERSITY OF FLORIDA

EAFTC Software Architecture

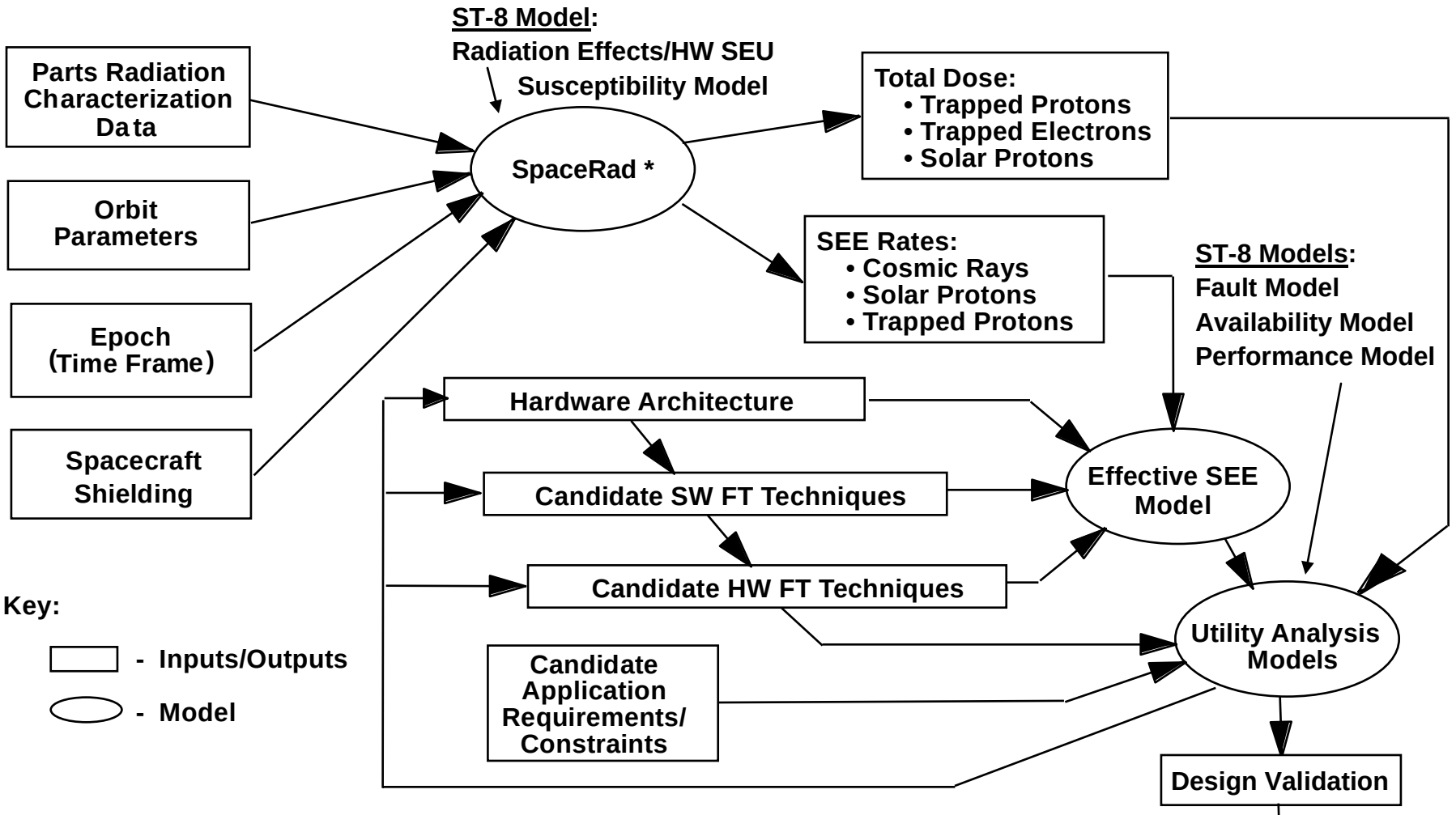
Honeywell



Addresses Technology Advance components A, B, and C

Methodology for Migrating COTS Technology to Space

Honeywell



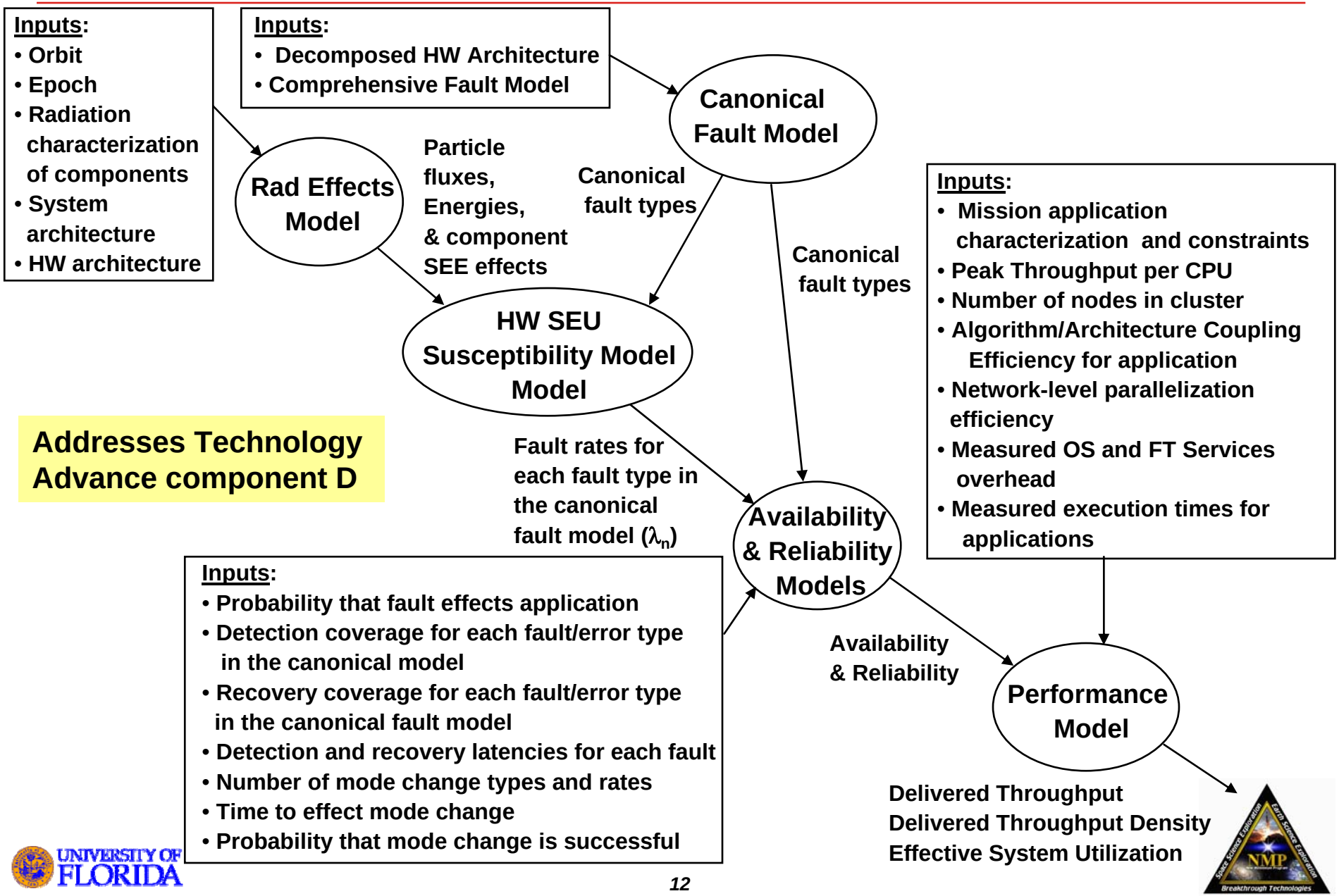
* The Space Rad tool which includes multiple earth magnetic field and solar activity models

Addresses Technology Advance component D

UNIVERSITY OF FLORIDA

EAFTC Model Flow

Honeywell

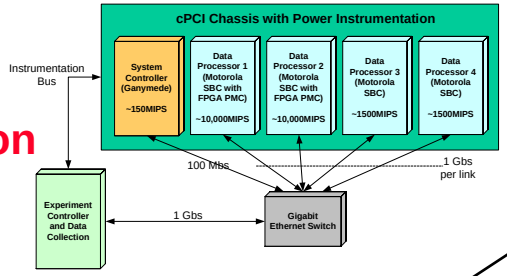


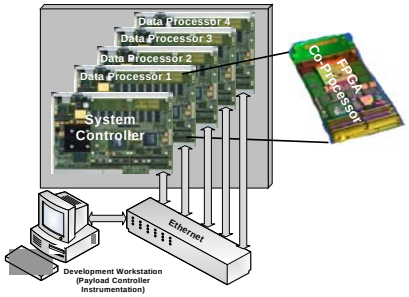
UNIVERSITY OF FLORIDA

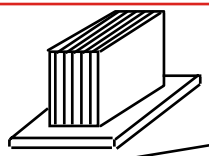
EAFTC Technology Advances to TRL7 Flight Experiment

Honeywell

Increasing system fidelity & integration







TRL7 Technology Validation

TRL6 Technology Validation

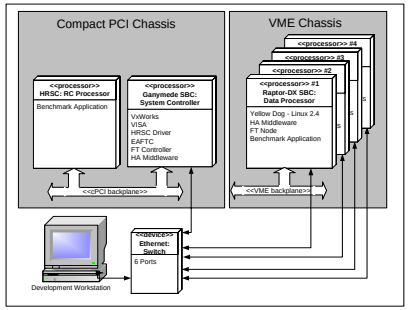
TRL5 Technology Validation

TRL4 Technology Validation

TRL4 Validation

- Demonstrated basic EAFTC technologies in a laboratory environment on COTS hardware testbed including radiation source and sensor
  - Environment Sensor
  - Alert Generator
  - High Availability Middleware
  - Replication Services

NASA adds requirement for fault-tolerant cluster and fault-tolerant MPI capability



TRL6 Validation

- Demonstrate enhanced EAFTC technologies in a laboratory environment on prototype flight hardware including exposure to radiation beam
- Validate and refine predictive models and predictive model parameters with experiment data
- complete set of canonical fault injection experiments

TRL7 Validation

- Demonstrate EAFTC technologies in a real space environment
- Validate predictive models and predictive model parameters with experiment data
- TRL7 experiments will be identical to those performed and rung out during TRL6 demonstration and validation

TRL5 Validation

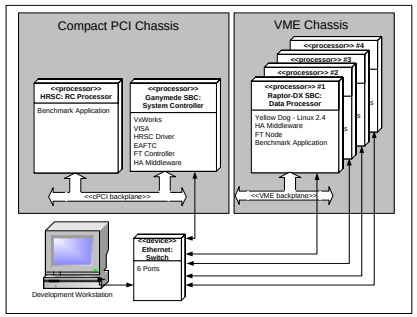
- Demonstrate basic EAFTC technologies in a laboratory environment on testbed hardware with partially integrated Fault Tolerance Services
- Develop predictive models
- Validate and refine predictive models and predictive model parameters with experiment data
- partial set of canonical fault injection experiments

UNIVERSITY OF FLORIDA

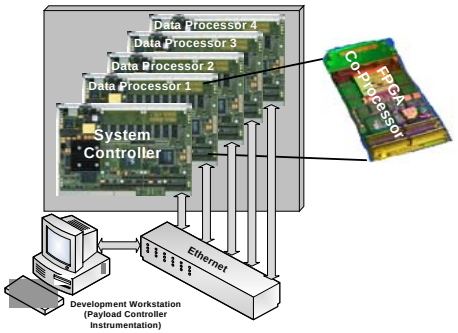
Technology Validation Plan

Honeywell

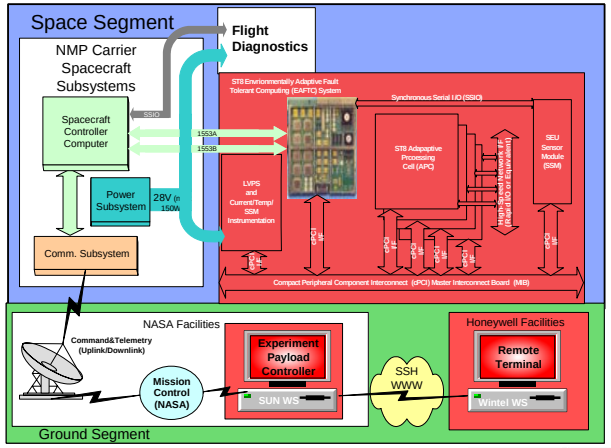
- **Three prototype systems will be implemented**
  - the prototype systems will implement the EAFTC architecture in both hardware and software domains
  - P4, P5, and P6 systems will be used to perform TRL4, TRL5, and TRL6 respectively
  - used for software development and test
- **The final ground based system configuration will consist of the space-qualified flight system**
  - called Flight 1 (F1)
  - will be used to perform final software tests
  - will be used in flight for TRL7 demonstration and validation



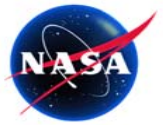
P4



P5 and P6



F1



Honeywell

EAFTC Flight System

UNIVERSITY OF FLORIDA

ST-8 EAFTC Level 1 Requirements

Honeywell

The EAFTC High Performance COTS Computing Experiment shall validate that the technology is capable of:

- **Providing a minimum of 100 MIPS/Watt of sustained general purpose parallel processing throughput when applied to scientific data processing in the nominal (non-solar flare) LEO and GEO natural space radiation environments (Requirement 1.0-1)**

- **Providing 0.995 reliability and 0.995 availability over a 5 year mission in LEO and GEO environments by applying the data obtained during the in-space validation experiment to the system models developed during the formulation refinement and implementation phases (Requirement 1.0-2)**

Rationale: **If EAFTC technology is to be successful, the primary service it must deliver high throughput density (MIPS/watt) to the science application with high reliability and high availability. In order for EAFTC technology to be of interest to the science community, it must provide at least 10X the throughput density of an alternative radiation tolerant system. Providing high throughput density alone is insufficient. Providing high throughput density with low availability delivers low effective system utilization to the application. The system must be able to meet the reliability requirements for a long term, i.e., at least a 5-year, science mission. EAFTC technology must be applicable to wide variety of future mission applications.**

UNIVERSITY OF FLORIDA

Relevant Space Environments

Honeywell

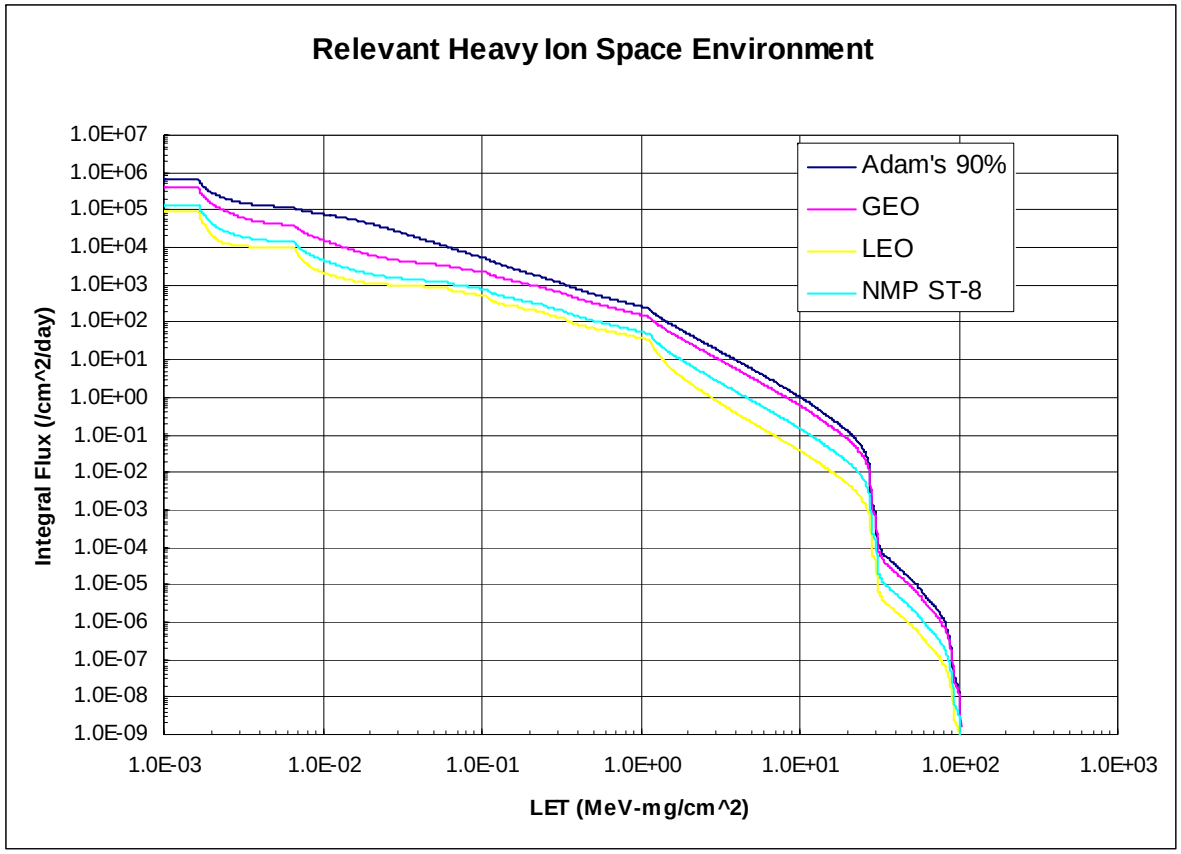
Space Environment	Orbit Parameters (Apogee x Perigee x Inclination)	Heavy Ion	Proton	Rationale
GEO	35,790 km x 35,790 km x 0 °	Major contributor to SEU rate	Low	Common orbit with a consistent environment
Deep Space (interplanetary space)	Beyond Geo	Assume same as GEO	Low	We will use GEO for deep space assessments
LEO	1470 km x 1470 km x 53°	Moderate	Rich proton and electron due to Van Allen Belts.	Trapped belt exposure; stressing proton environment
ALSF (Solar Flare)	Will use GEO for maximum exposure	High	High	Worst case environment for long term space missions
NM ST-8 (proposed) *	1400 km x 300 km x 70 ° - 90 °	Moderate at Apogee Low at Perigee	Moderate at Apogee Absent at Perigee	NMP ST-8 experiment orbit. Representative of varying proton and heavy ion fluxes

* Selected by NASA to maximize EAFTC experiment data collection

UNIVERSITY OF FLORIDA

Relevant Space Environment – Heavy Ion Spectrum

Honeywell

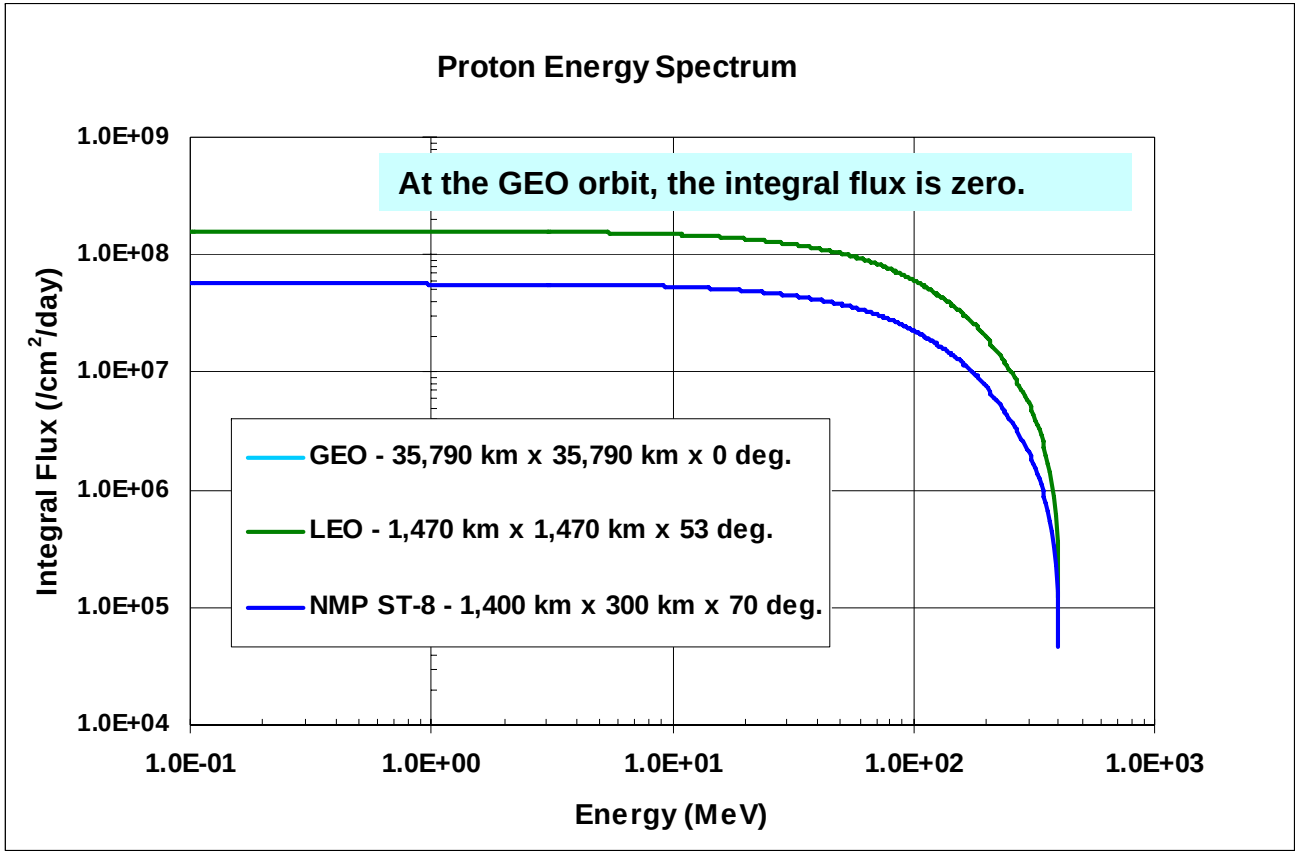


Adam's 90% Worst Case encompasses the other candidate environments including LEO, GEO, and the NMP ST-8 elliptical 300km x 1400 km orbit at 70° inclination, and will be used to drive the EAFTC Flight Experiment Payload design for a heavy ion environment

UNIVERSITY OF FLORIDA

Relevant Space Environment - Proton Energy Spectrum

Honeywell



The 1470km orbit is the selection for ST-8 proton design criterion since it is an upper bound of the other candidate environments.

UNIVERSITY OF FLORIDA

Relevant Space Environment ST-8 Mission Orbit

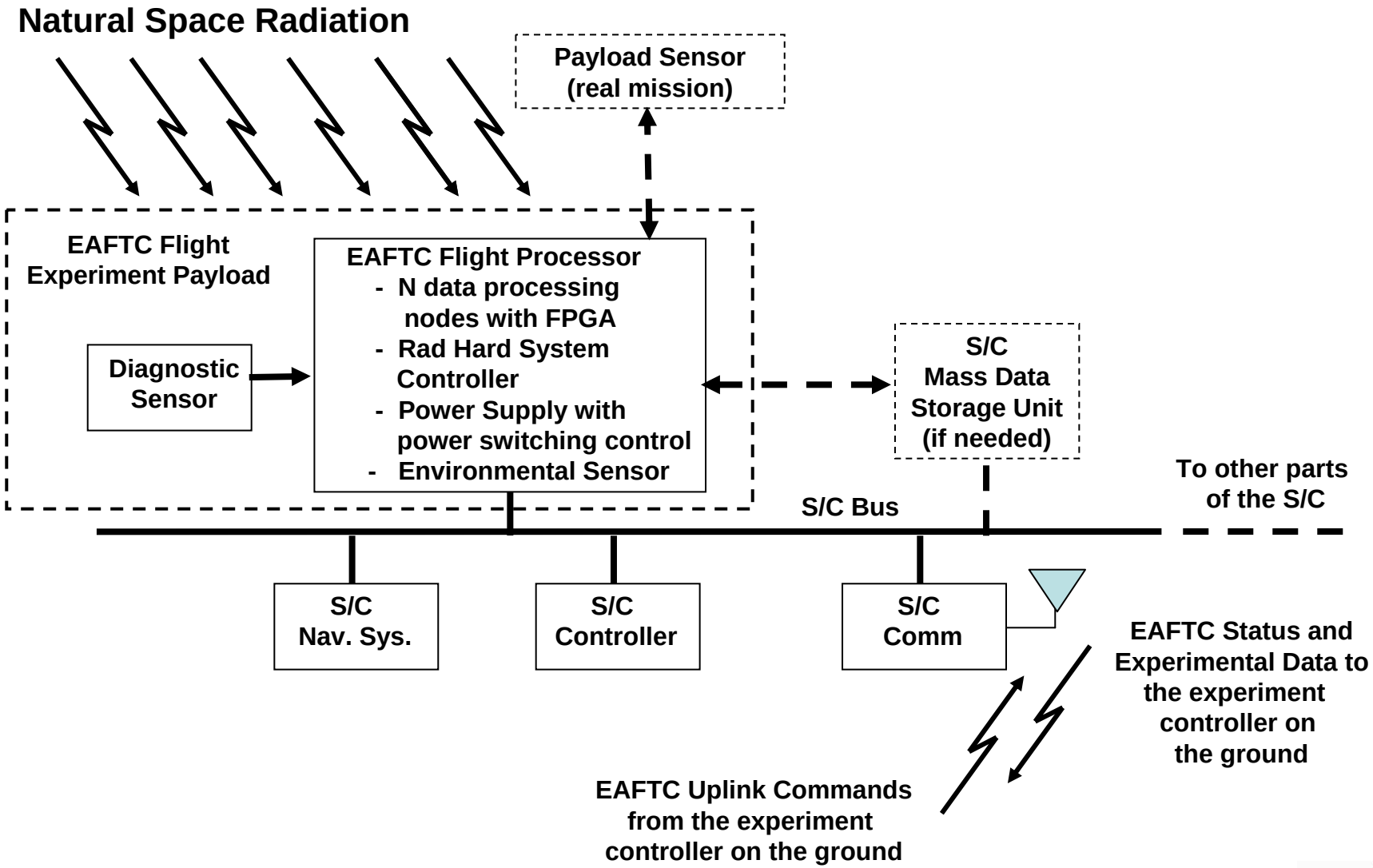
Honeywell

- Based upon radiation effects analysis completed to date, >6000 upsets are expected in the proposed 4-month EAFTC flight experiment
  - >50 upsets per day
- Three candidate science applications are being considered for the flight experiments: 2D FFT, LU Decomposition, science application NASA GFSC Developed for the REE program
  - all of these applications can be tailored to: 1) stress the EAFTC system, and 2) fit within the hardware capabilities of the EAFTC Flight Experiment Payload

UNIVERSITY OF FLORIDA

EAFTC Flight Experiment Configuration

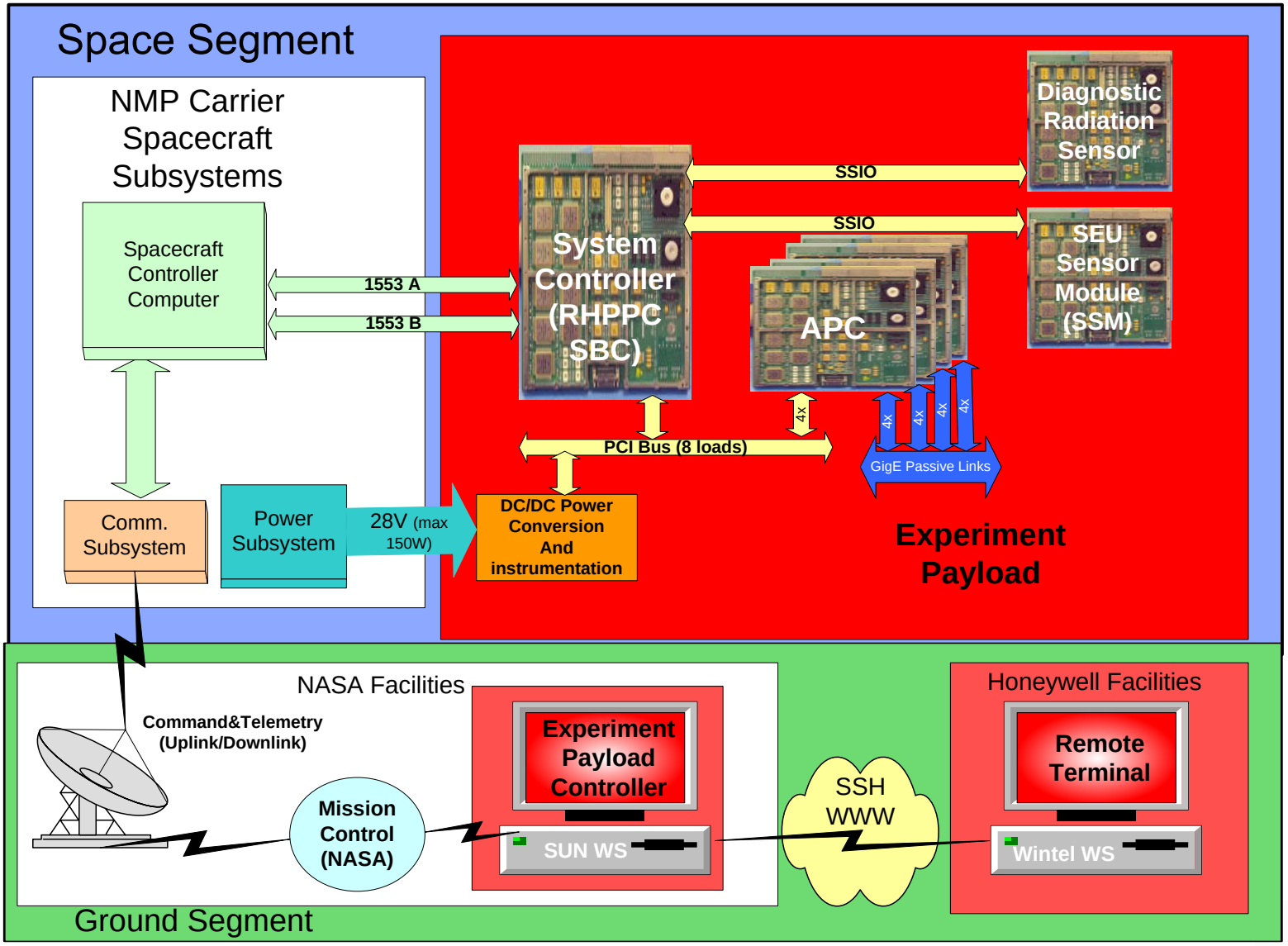
Honeywell



Addresses Technology Advance components A, B, C, and D

Experiment System

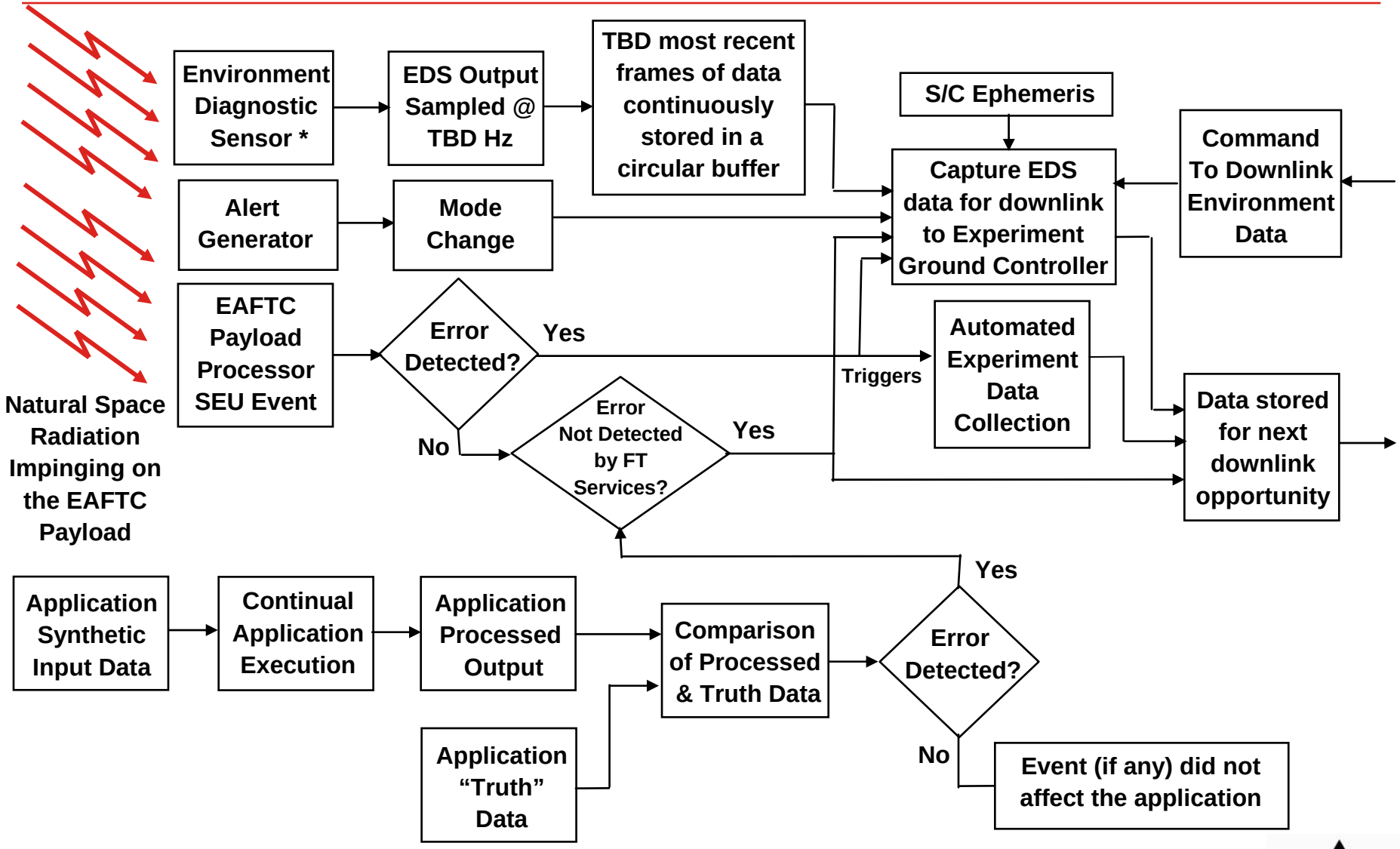
Honeywell



UNIVERSITY OF FLORIDA

SEU Fault Tolerance Experiment Data Collection

Honeywell

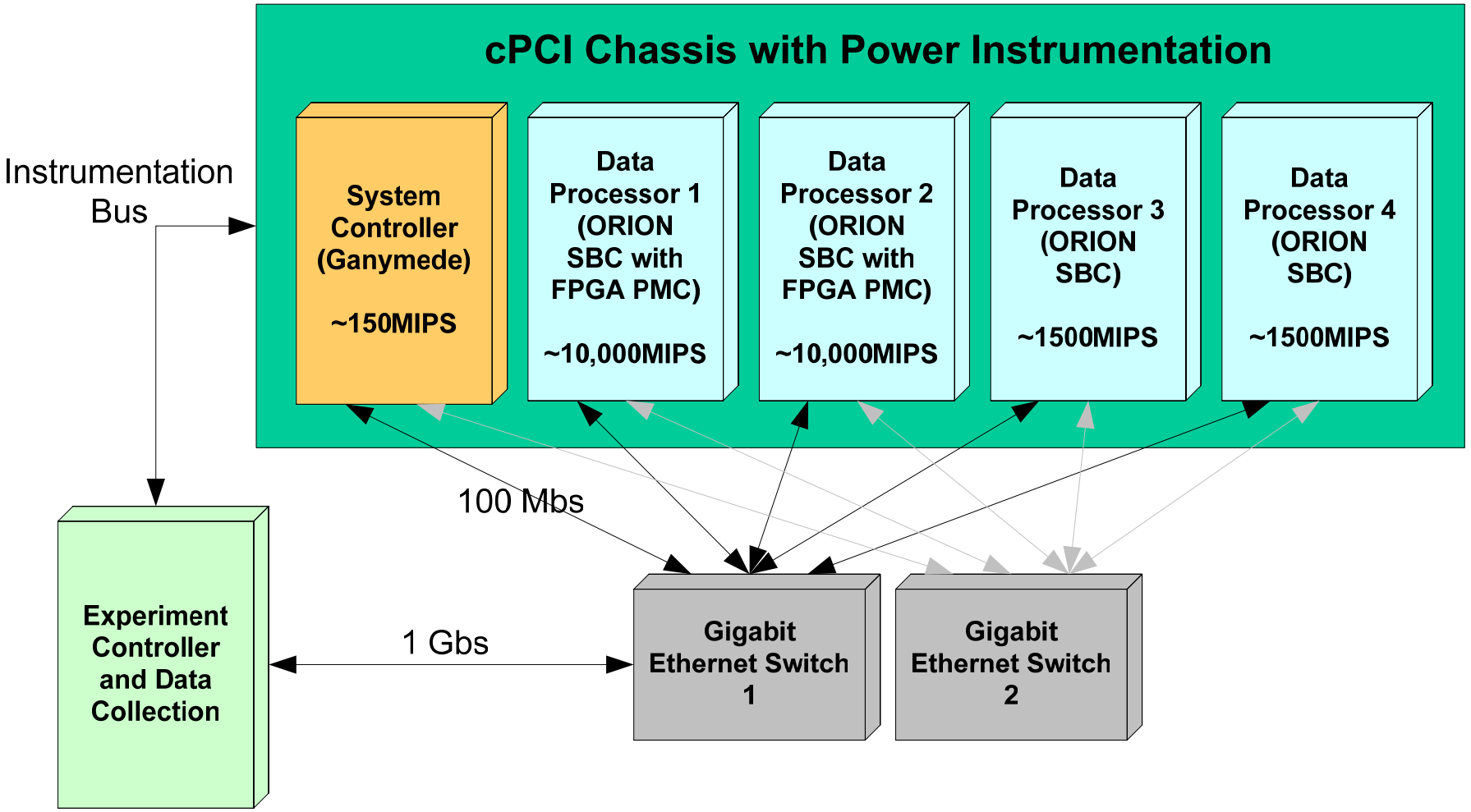


* The Experiment Diagnostic Sensor is not part of the EAFTC technology validation. It is needed for correlation of the occurrence of SEU events and the radiation environment, and for calibration of the Radiation Effects/HW SEU Susceptibility Models

UNIVERSITY OF FLORIDA

TRL5 Hardware Architecture

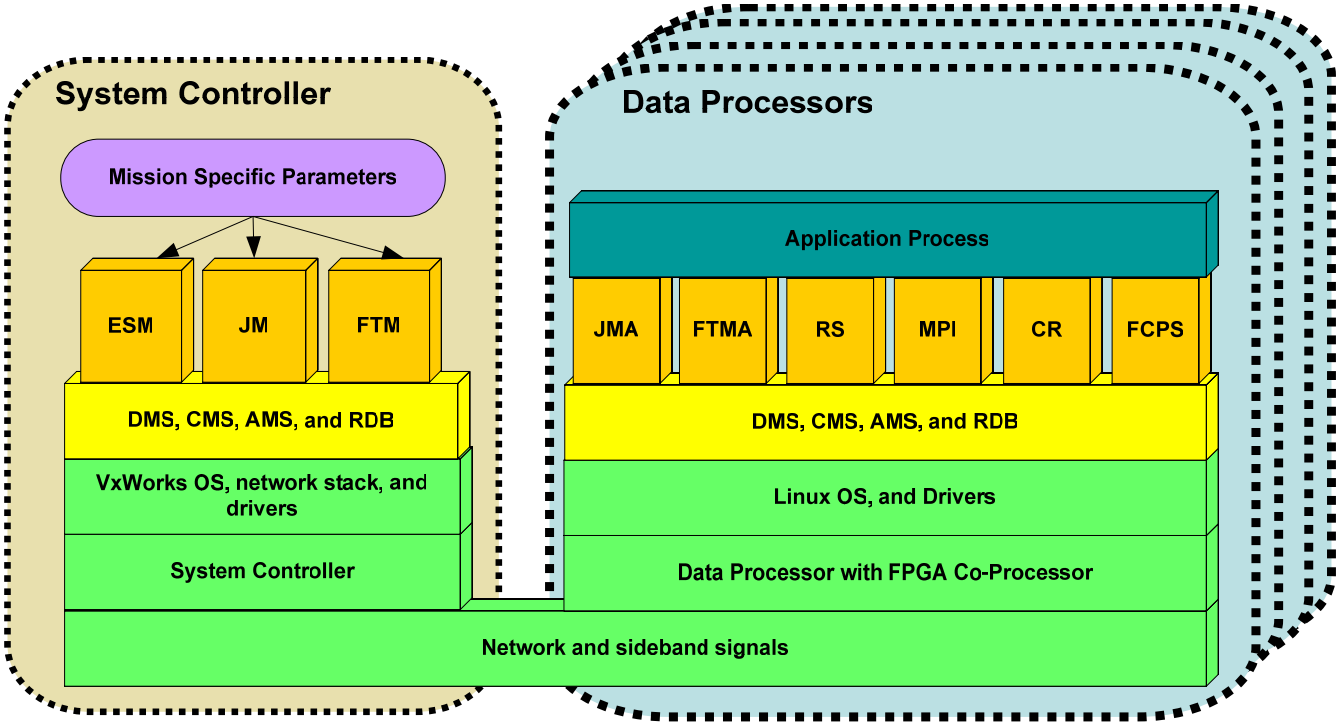
Honeywell



UNIVERSITY OF FLORIDA

EAFTC Software Architecture (TRL5+)

Honeywell



- Mission Specific Components
- EAFTC Specific Components
- High Availability Middleware (HAM) Components
- Platform Components
- Application Components

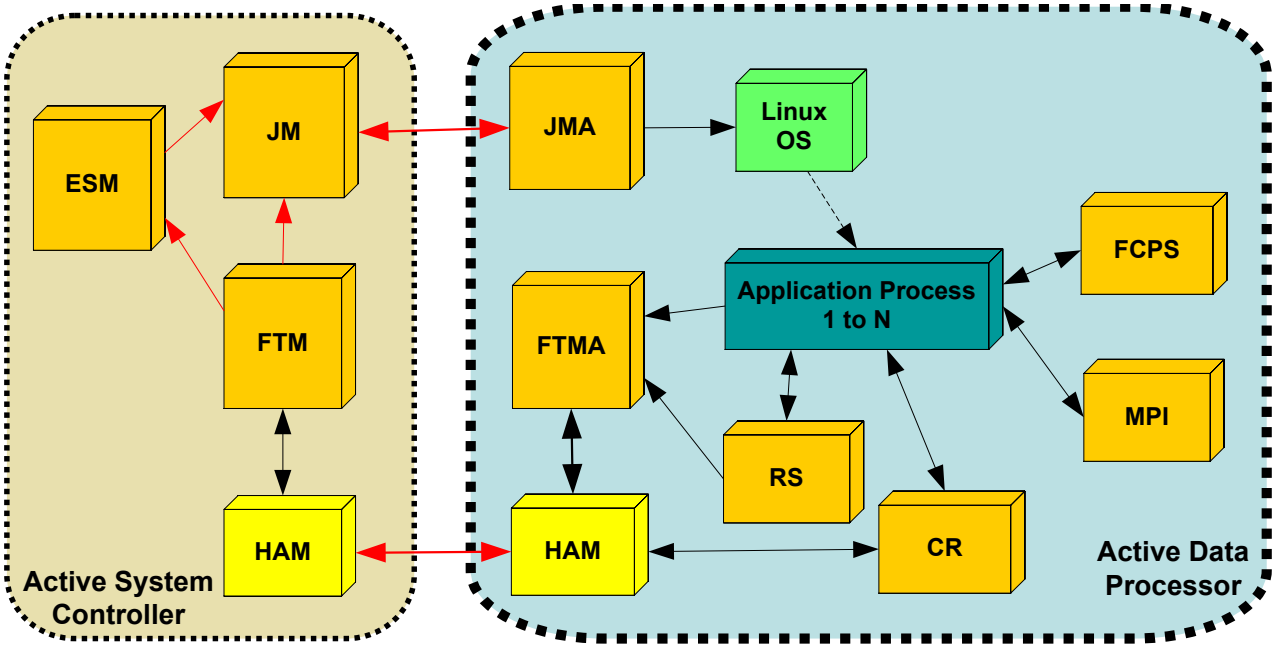
ESM – Environmental Sensor Monitor
JM – Job Manager
JMA – Job Management Agent
FTM- Fault Tolerance Manager
FTMA – Fault Tolerance Management Agent
RS – Replication Services
MPI – Message Passing Interface
FCPS – FPGA Co-Processor Services
CR – Checkpoint and Rollback
CMS – Cluster Management Services
AMS – Availability Management Services
DMS – Distributed Messaging Services
RDB – Replicated Database

UNIVERSITY OF FLORIDA

EAFTC Software Components Collaboration

Honeywell

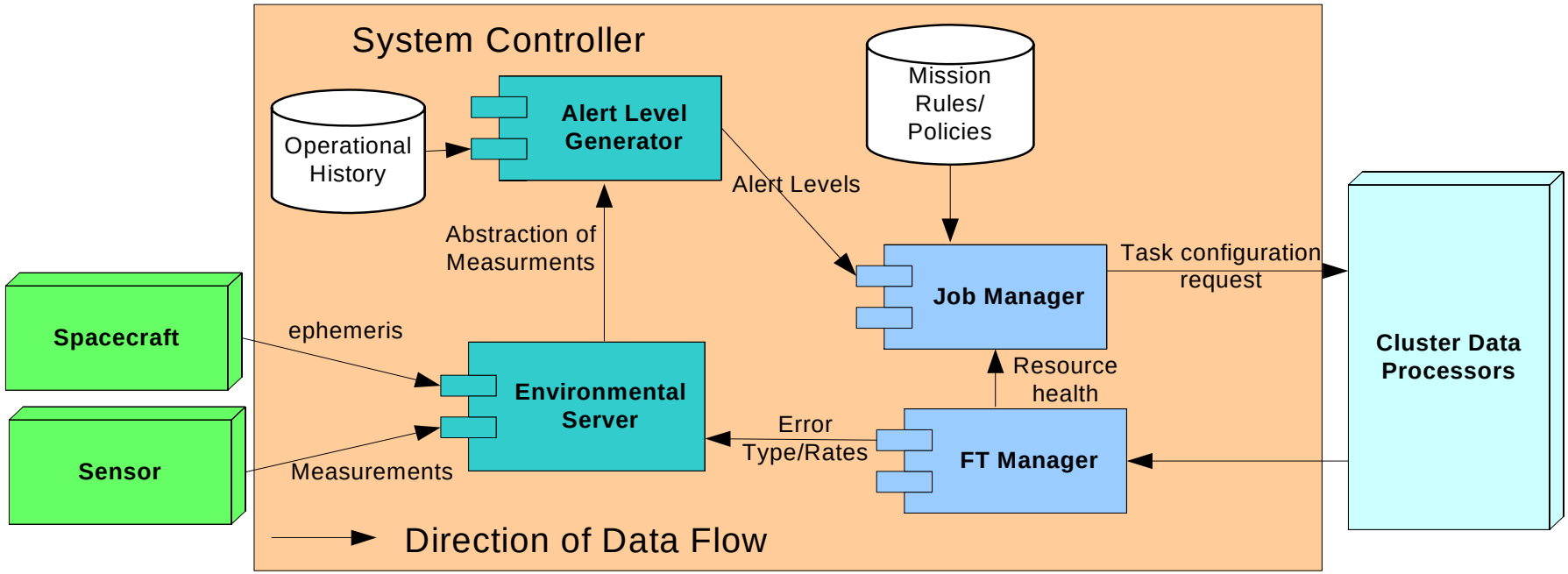
- **EAFTC Middleware Components**
  - Environmental Sensor Monitor (ESM)
  - Job Management Services (JMS)
    -- Job Manager (JM) + Job Management Agent (JMA)
  - Fault Tolerance Management Services (FTMS)
    -- Fault Tolerance Manager (FTM) + Fault Tolerance Management Agent (FTMA)
  - High Availability Middleware Services (HAM)
  - Message Passing Interface (MPI)
  - FPGA Co-Processor Services (FCPS)



Links in Red are HAM DMS based communication links.

Environment Sensor Manager

Honeywell



Status

Honeywell

- **Successful TRL 4 demonstration for ST-8 Phase A TMA (Technology Maturity Assessment)**
  - parallel processing platform with FPGA co-processor acceleration
  - environmental adaptivity
    - -- environmental sensing alert generation & response
    - -- replicated services (SCP, TMR, etc.)
    - -- application/process priority
    - -- system operating mode
- **Successfully passed TRL5 E-SRR (Experiment – Systems Requirements Review) gate**
- **Successfully demonstrated the easy porting of HA Middleware on a number of platforms with a variety of PPC engines (750FX, 970, & 603e) with VxWorks and a variety of Linux OS (Monta Vista, Yellow Dog, Red Hat)**
  - conducted several demonstrations, e.g.,
    - -- checkpoint and fail-over model
    - -- checkpoint and fail-over application on active, standby, and unassigned nodes

UNIVERSITY OF FLORIDA

Future Plans

Honeywell

- Get through the normal TRL5 NMP “gates” to move on to Phase C (Implementation Phase)
- TRL5 spiral development and testing
  - emphasis on high performance fault-tolerant cluster processing
  - SWIFI (Software Implemented Fault Injection)
  - addition of ABFT (Algorithm-Based Fault Tolerance) capability
- Conduct successful TRL5 TMA demonstration
- Radiation characterization of key, but as yet untested, COTS components
  - processing node bridge ship
  - high performance network switch

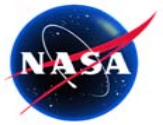
UNIVERSITY OF FLORIDA

Summary & Conclusion

Honeywell

- **Environmental adaptivity encompasses more than responsiveness to the radiation environment**
  - **functional criticality**
  - **application/process priority**
  - **system operating mode**
- **Environmental adaptivity is only a part of EAFTC technology**
- **Focus of Phase B EAFTC technology development is on high performance, fault-tolerant cluster processing for science applications**
- **EAFTC technology is equally applicable to other application domains**
  - **rovers**
  - **landers**
  - **UAVs**
  - **rad hard space applications**
- **Unlike previous attempts to migrate high performance COTS processing to space (Space Touchstone, REE, ISAC), the NMP ST-8 program has "legs"**
  - **NASA NMP is providing the ride**
  - **Orbital Science Corporation has been selected to be the S/C provider**
  - **Pegasus has been selected as the launch vehicle**

UNIVERSITY OF FLORIDA



References (1 of 3)

Honeywell

[1] Ramos, Jeremy, and D. Brenner, "Environmentally-Adaptive Fault Tolerant Computing (EAFTC): An Enabling Technology for COTS based Space Computing ," *Proceedings of Proceedings of the 2004 IEEE Aerospace Conference*, Big Sky, MN, March 8-15, 2004.

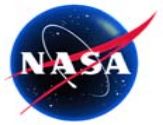
[2] Samson, Jr. John R., "Migrating High Performance Computing to Space," 7th High Performance Embedded Computing Workshop, M.I.T. Lincoln Laboratory, September 22, 2003.

[3] Samson, Jr., John R., "Space Touchstone Experimental Program (STEP) – Final Report 002AD," January 15, 1996.

[4] Karapetian, Arbi, R. Some, and J. Behan, "Radiation Fault Modeling and Fault Rate Estimation for a COTS Based Space-borne Computer," *Proceedings of Proceedings of the 2002 IEEE Aerospace Conference*, Big Sky, MN, March 9-16, 2002.

[5] Some, Raphael, W. Kim, G. Khanoyan, and L. Callum, "Fault Injection Experiment Results in Space Borne Parallel Application Programs," *Proceedings of Proceedings of the 2002 IEEE Aerospace Conference*, Big Sky, MN, March 9-16, 2002.

UNIVERSITY OF FLORIDA



References (2 of 3)

Honeywell

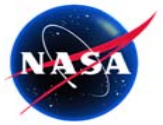
[6] Some, Raphael, J. Behan, G. Khanoyan, L. Callum, and A. Agrawal, "Fault-Tolerant Systems Design Estimating Cache Contents and Usage," *Proceedings of Proceedings of the 2002 IEEE Aerospace Conference*, Big Sky, MN, March 9-16, 2002.

[7] Lovellette, Michael, and K. Wood, "Strategies for Fault-Tolerant, Space-Based Computing: Lessons Learned for the the ARGOS Testbed," *Proceedings of Proceedings of the 2002 IEEE Aerospace Conference*, Big Sky, MN, March 9-16, 2002.

[8] Samson, Jr., John R., and C. Markiewicz, "Adaptive Resource Management (ARM) Middleware and System Architecture – the Path for Using COTS in Space," *Proceedings of the 2000 IEEE Aerospace Conference*, Big Sky, MN, March 8-15, 2000.

[9] Samson, Jr., John R., L. Dela Torre, J. Ring, and T. Stottlar, "A Comparison of Algorithm-Based Fault Tolerance and Traditional Redundant Self-Checking for SEU Mitigation," *Proceedings of the 20th Digital Avionics Systems Conference*, Daytona Beach, Florida, 18 October 2001.

UNIVERSITY OF FLORIDA



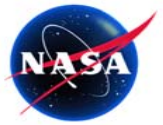
References (3 of 3)

Honeywell

[10] Samson, Jr., John R., "SEUs from a System Perspective," Single Event Upsets in Future Computing Systems Workshop, Pasadena, CA, May 20, 2003.

[11] Prado, Ed, J. R. Samson, Jr., and D. Spina. "The COTS Conundrum," *Proceedings of the 2000 IEEE Aerospace Conference*, Big Sky, MN, March 9-15, 2003.

UNIVERSITY OF FLORIDA



Acknowledgement

Honeywell

The Environmentally Adaptive Fault-Tolerant Computing effort is funded under NASA NMP ST-8 contract NMO-710209.

UNIVERSITY OF FLORIDA