High Availability Controls

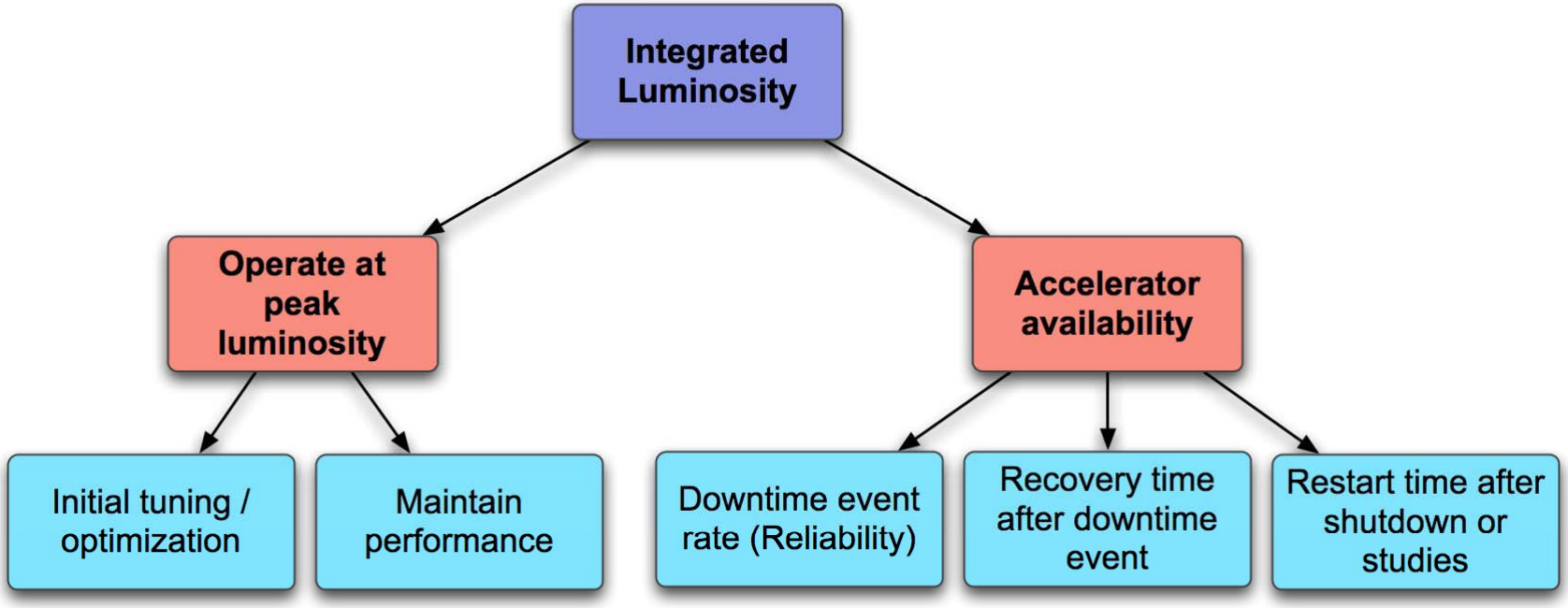
Kevin M. Krause
Fermilab

High Availability Controls Goal

Support ILC accelerator availability goal of 85%.

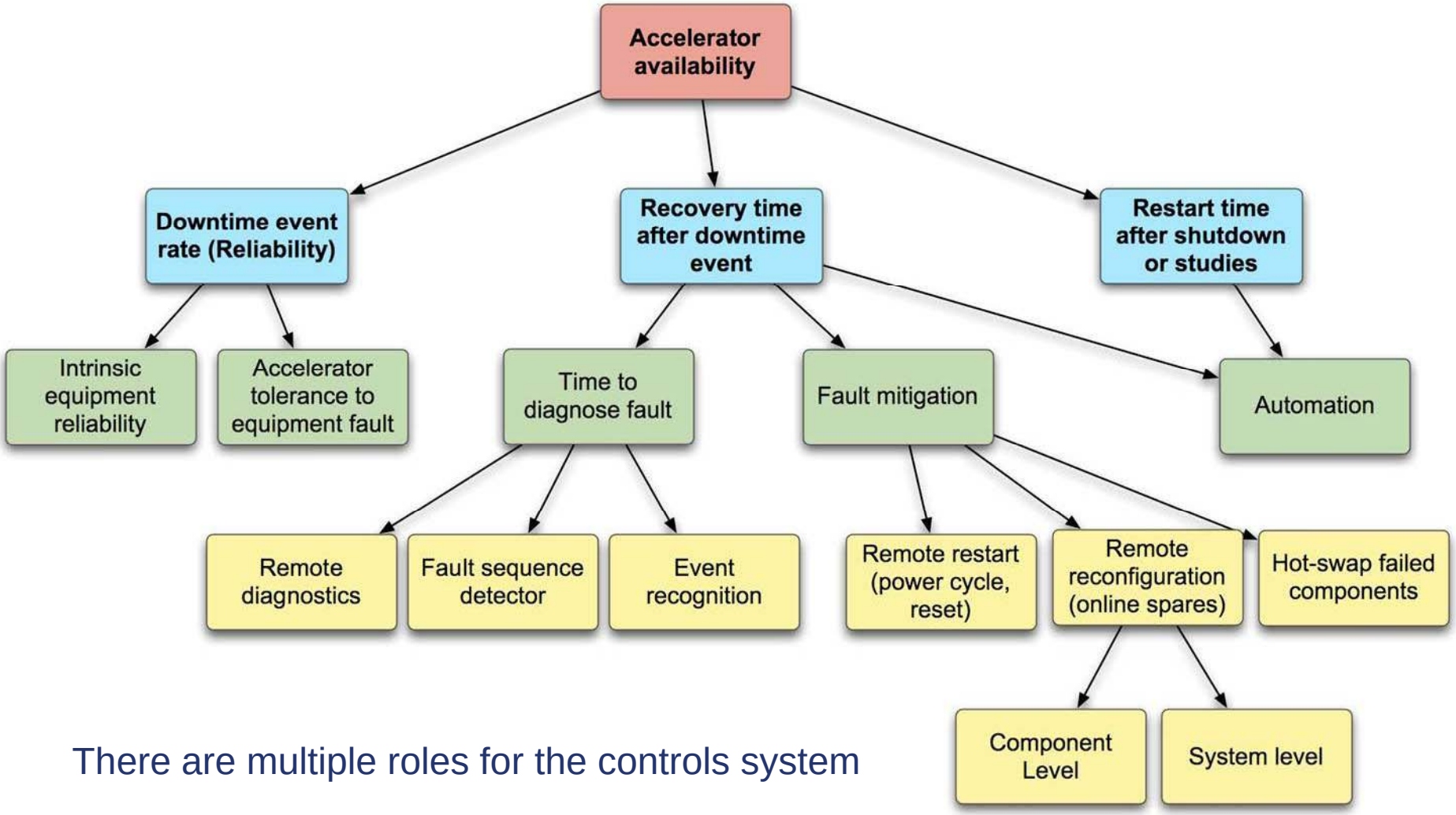
- Intrinsic control system availability of 99% by design.
- Functionality to minimize overall accelerator downtime.

Accelerator Availability Considerations



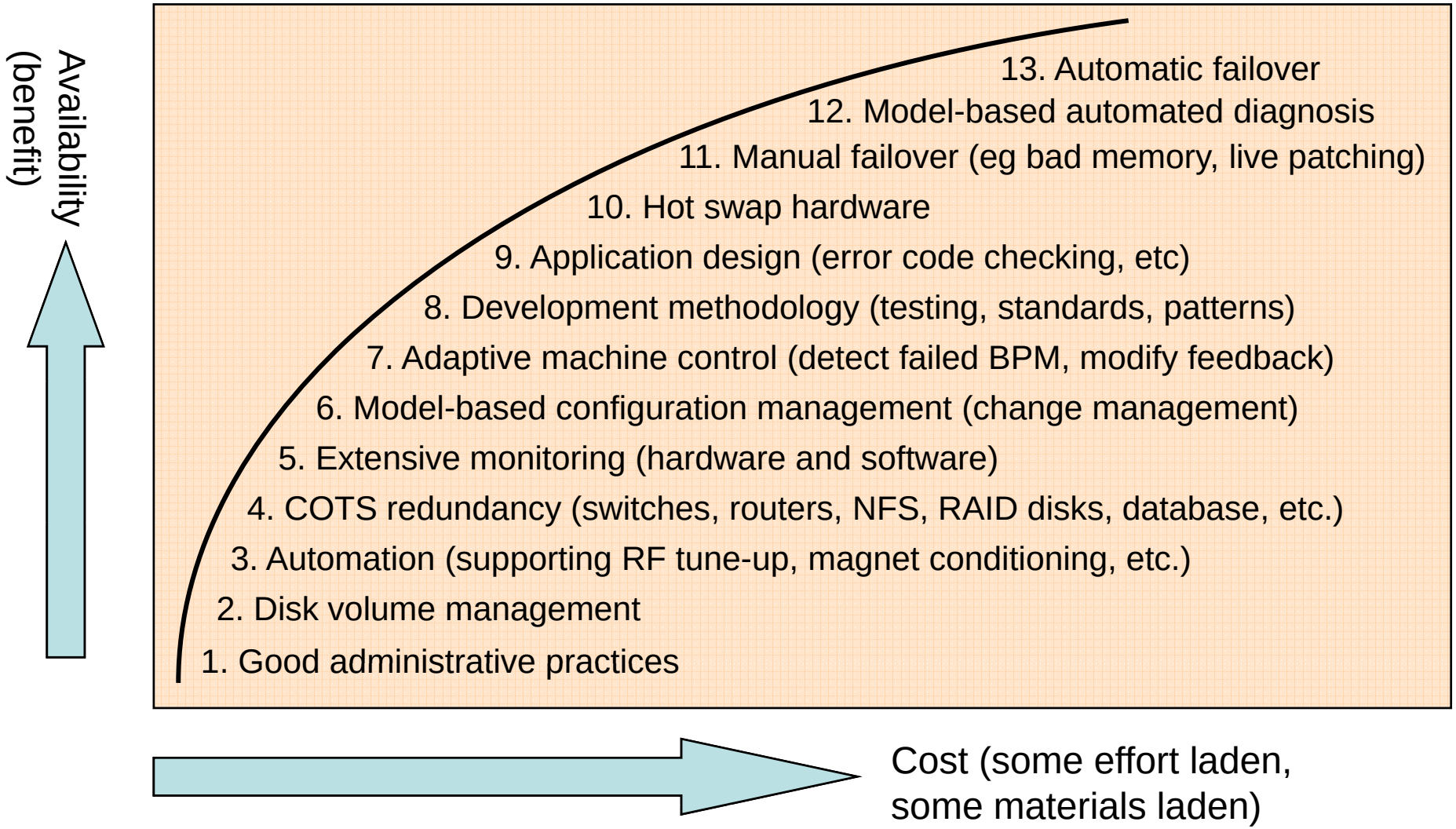
Availability is a function of intrinsic reliability (Mean Time Between Failures) and speed of return to service (Mean Time To Repair).

Accelerator Availability Considerations



There are multiple roles for the controls system

Cost/Benefit Analysis



Cost/Benefit Analysis

- Evaluate techniques by Cost/Benefit to establish order. We will need to understand:
  - Controls system and accelerator-wide failure modes.
  - Which techniques mitigate which failure modes.
  - Total cost of employing a technique.
- Use understanding to refine and enhance our techniques “arsenal.”
- Certain techniques will require R&D.
- We will need to establish a Cost/Benefit order and complete R&D on techniques for EDR.

High Availability Controls R&D Objectives

- Learn about High Availability in context of accelerator controls.
- Develop and/or adopt a methodology for examining control system failures.
- Develop techniques for detecting and managing identified failure modes.
- Develop a full “vertical” prototype implementation and integrate portions with test stands.
- Leverage the Availism simulation to evaluate our failure analysis and its impact on controls availability.
- Acquire enough experience and data to construct a plan that achieves the controls availability goal.

High Availability Controls Status

- Many ATCA platforms under investigation
  - New instrumentation & controls designs for both ATCA and µTCA.
  - DESY evaluating ATCA for XFEL Controls
  - UIUC specifying ATCA carrier card to host VME cards.
  - EPICS ported to ATCA CPU blades running Linux.
  - Demonstrated basic redundancy and failover with EPICS.

High Availability Controls Status

- Software investigations
  - Exploring ATCA from a control system software perspective.
  - Exploring High Availability solutions for control system software.
  - Identified several candidate High Availability frameworks

High Availability Controls R&D Directions

- Software
  - Integrate existing core controls software components with Telecom High Availability framework.
  - Evaluate monitoring/management standards and their application to controls.
- Hardware
  - Leverage features offered by AdvancedTCA and microTCA.
  - Integrate diagnostic functions with technical equipment.
  - Accommodate remote access and remote control.

High Availability Controls R&D Directions

- System
  - Execute Failure Mode Analysis.
  - Develop fault detection algorithms.
  - Develop a model-based framework for automated diagnostics.
  - Integrate Configuration Management of all software and hardware components.
  - Develop conflict avoidance strategies.
  - Identify and select development and QA methodologies.

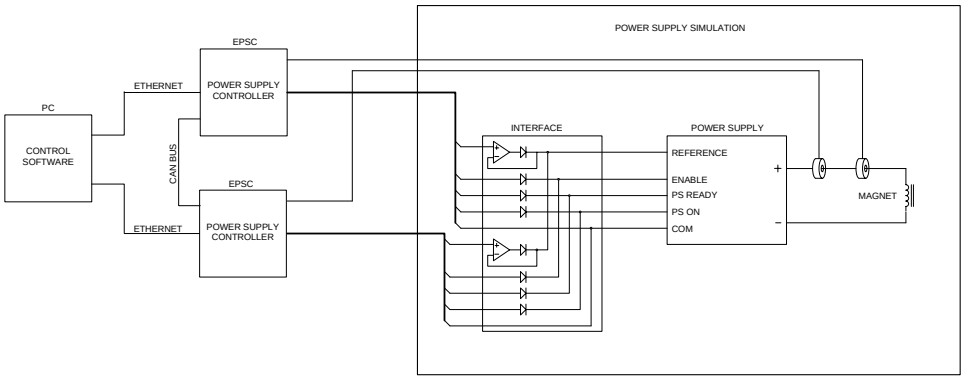
High Availability Controls Work Packages

- Failure Mode Analysis.
- High Availability Process Variable Gateway.
- System monitoring and management.
- Model-based automated diagnostics.
- Model-based control system configuration management.
- Electronics platform evaluation and development.
- Design development plan.

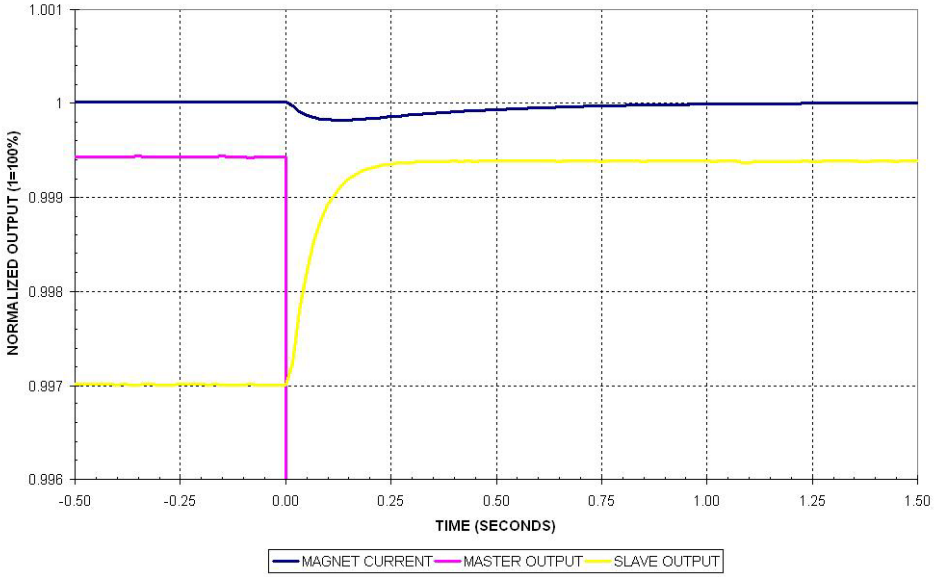
Open Questions

- Who owns high availability goals?
- Who owns detection algorithms?
- To what degree do failure mode analysis and R&D on techniques interact?
- How to collaborate on High Availability R&D across regions?
- How to integrate High Availability R&D into test facilities effectively?
- When will we be confident enough to document a plan that meets availability goal?

3.2.1 Progress: HA Dual Control



REDUNDANT POWER SUPPLY CONTROLLER SWITCHOVER TRANSIENT



- Magnet PS Controller Failover Demo
  - **Master, Slave controllers w/ CANbus link for synchronization**
  - **Digital regulation by PI control**
  - **Either unit can be designated Master**
  - **Master updates slave @ 120 Hz**
  - **Slave tracks Master until master fails (simulated by interlock trip)**
  - **Simulated magnet current dipped <.02% as slave smoothly assumes control, output settles in ~0.75 seconds**
- Importance
  - **This experiment (along with hot-swap of failed controller) demonstrates that normal 1-2 hr MTTR to swap a controller can be eliminated**
  - **Overall PS system goal is A>99%**
  - **Availability limited to <90% without redundant bulks and controllers**
  - **RETURN**

Control System high availability

High availability is achieved through the application of a variety of well-known techniques. Within this work package we research the application of these techniques where the application to controls is not well understood. Among the techniques to apply are conflict avoidance, controller redundancy and failover, model-based resource monitoring, model-based configuration management, automated diagnosis, and adaptive control. The goal is to create an operational example of selected techniques applicable to the ILCTA.

This task covers the evaluation, selection or development of modular instrument standards for both the control system and front end instrumentation for the ILC. Both hardware and software systems are new concepts which must be thoroughly investigated an adapted to our needs. The issues are challenging since managing the system will become very software-intensive. The ultimate goal is redundant systems where single points of failure are minimized and up-time can be guaranteed. The goal is to develop tools for other labs to use in test systems such as the SRF facility at FNAL.

The controls collaboration studying architectures is broad and includes major labs in the US, Japan and Germany. UIUC is conducting evaluations as part of a larger evaluation plan with SLAC, ANL and FNAL. FNAL and ANL will provide local supervision for the UIUC group.

Two Labs are funded for this work package (Argonne and Fermilab). Argonne will provide overall leadership for the work package.

Electronic platform development for ILC application

The ILC will not run with the required availability without a much stronger control system than present machines. Commercial products now offer products designed for high availability (0.99999 for a loaded crate) are being investigated for applicability in both areas.

To this end, the ILC Controls Global Systems Group has begun investigations into the new commercial standard modular processor architecture (ATCA) designed for High Availability systems in the range of that required for the ILC. Some of the features that make it attractive as an alternative to more commonly used hardware platforms (VME, VXI, etc) include: redundant power sources and backplane, remote power up/power down of modules, hot swap, module self-identification, a “Shelf Manager” for intelligently managing resources, and high speed point-to-point serial links within the crate for redundancy and higher performance than traditional parallel bus backplanes. The standard is still new and to date the platform has not been deployed in accelerator controls and instrumentation environments. Investigate the suitability of the Advanced Telecom Computing Architecture (ATCA) as the standard large and small form-factor electronics platforms. This includes both hardware and software suitability. Also included is an investigation of telecom equipment management standards (such as DTMF CIM and SNMP), and their suitability for managing controls front ends.

Continue examination of full ATCA and micro-TCA for hosting electronics. Evaluate analog performance of subsequent board revisions. Evaluate connector design for ATCA and micro-TCA. Investigate integration issues between COTS ATCA boards (such as switches and CPU’s) and custom developed boards. Evaluate the suitability of telecom management standards, including DTMF CIM specifications for unifying management of all field electronics. Port EPICS to ATCA CPUs with databases and drivers to run candidate I/O boards. Develop a prototype interface for shelf management using telecom management standards.

This Work Package expands on the scope of work performed under a previous work package, “*HA Standard Modules for Instrumentation*” funded through FY07.

Three Labs are funded for this work package (Fermilab, Argonne, and SLAC). Fermilab will provide overall leadership for the work package.

Control system architecture

This involves researching and documenting the overall control system architecture. Included here are the site-wide network infrastructure, client applications tier, services tier, technical equipment tier, and protocols. In addition, the set of standards, interfaces, and methodology are to be documented. Unique research is required to assure that the requirements for high availability, scalability, automation, feedback, synchronous operation, and remote operation are met with an optimized design.

Two Labs are funded for this work package (Fermilab and Argonne). Fermilab will provide overall leadership for the work package.

R&D program for HA

- Configuration management, QA, etc will be essential for success once the ILC reaches the project phase.

- In the mean time, we need to become better equipped to make sound technical and cost-conscious design decisions
  - **Learn what it takes to implement HA technical solutions.**
  - **Evaluate payback and cost / penalty.**
  - **Evaluate graded (measured) implementation and applicability.**

- HA R&D targets electronic systems (hardware, firmware, software)
  - **HA PS (and kicker) - N+M redundancy schemes.**
  - **Controls architecture, software 'ecosystem', availability management.**
  - **Evaluation of ATCA electronics platform (more than just HA).**