High Availability Electronics Architectures & Standards for ILC

The Case for Five 9's

Ray Larsen

SLAC ILC Program

Outline

- I. High Availability Electronics Design
- II. New Industry Open Architecture
- III. Application to ILC
- IV. Need for Standards
- V. Recommendations
- VI. Conclusions

I. HA Design Motivation

- Overall Machine Availability
  - ILC High Availability design critical due to unprecedented size, complexity and high cost of an idle machine. (Opportunity Cost of ILC ~$100K/hr.)
  - T. Himel Availability Collaboration[1] study has strongly demonstrated that ILC cannot be built in same manner as old machines or it will never work.
  - *Goal of this presentation is to show feasibility of subsystems with A approaching ideal A=1.*
  - Basic design tenets can be applied to *all* machine subsystems.

[1] *T. Himel & Collaboration Availability studies group*

High Availability Primer

- Availability A = MTBF/(MTBF+MTTR)
  - MTBF=Mean Time Before Failure
  - MTTR= Mean Time To Repair
  - If MTBF approaches infinity A approaches 1
  - If MTTR approaches zero A approaches 1
  - Both are *impossible* on a unit basis
  - Both *are possible* on a system basis.
- Key features for HA, i.e. A approaching 1:
  - Modular design
  - Built-in 1/n redundancy
  - Hot-swap capable at subsystem *unit* or *subunit* level

Historic HA Examples

- SLAC Modulators & Klystrons
  - 2 sectors out of 30 (16 out of 240 stations) or 6% were “hot spares” in original design
  - Beam energy maintained constant by hot-swap of standby station on pulse-by-pulse basis to recover station that tripped off for either klystron or modulator fault
  - M-K *System* operated very close to A=1.
  - At absolute max. energy where all stations used, no hot spares available, *A* dropped for every station trip.
- NIM-CAMAC-FASTBUS-VME-VXI
  - Quickly replaceable instrument modules minimize MTTR to just repair access time plus a few minutes to swap.
- Whole RF stations are hot-swap capable; current standard module designs are not.

NLC Flashback

- NLC proposed an overall target of A=0.85 (ZDR1996)
- ZDR defined 16 machine segments (systems) for both linacs
  - Assume each has 10 subsystems, or 160 total
    - Example subsystem: DR magnet power supplies
- Asub = (.85)**(1/160) = 0.998985 ~ 3-9's = 8.9 h/yr
  - Each subsystem on average is allowed a total downtime of ~ 1 shift/year.
  - If subsystem has 100 units, need 5-9's per unit implying a 100K hour MTBF.
- Feasible for very small but not for multi-KW units.

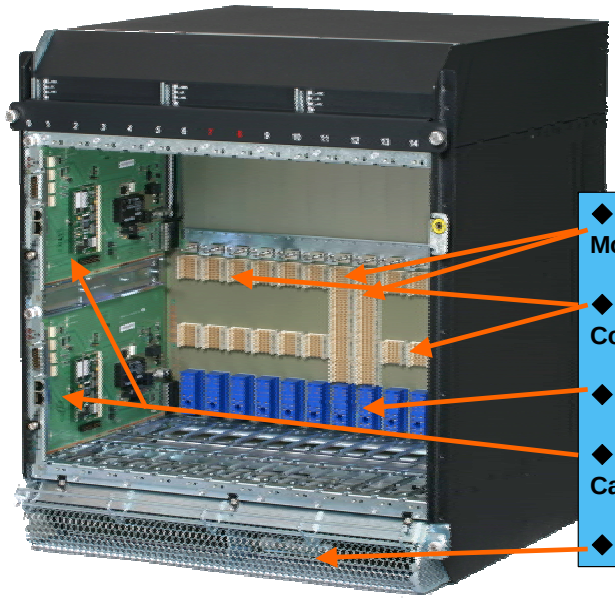
How High Availability?

- *As high as possible!* – Costs $100K/hr idle.
- A=0.85 gives away ~ $130M/yr.
- Consider a goal of 99% up-time, Atotal=0.99
- If electronics were the only issue, is this remotely thinkable?
- How well would various subsystems have to perform?
- With other systems limiting us like water, power, controls– is it reasonable to aim so high?

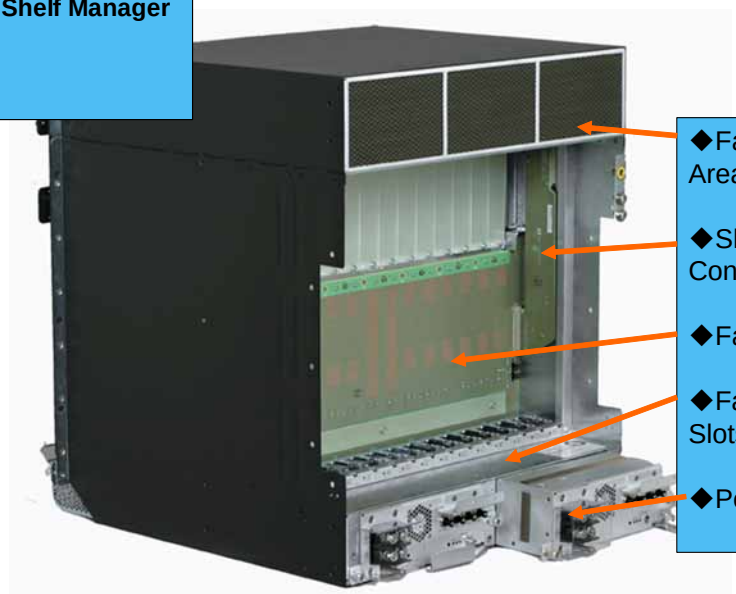
Consider A=0.99 Machine Goal

- Pretend all systems that keep machine off are electronic if you feel better.
- For 0.99 overall NLC, 1 subsystem must obtain Asub= (.99)**(1/160) = 0.999937 (0.55hr/yr)
- If subsystem has 100 power supplies, each supply would need A= 6- 9's, implying *1.6 million* hour MTBF.
- Obviously impossible if have to depend on MTBF alone.
- Industry shows: "*Man shall not live by MTBF alone.*"

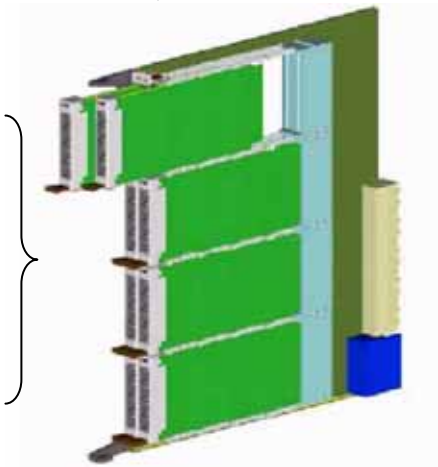
II. ATCA Telecom System: A=0.99999



- 2 Control & 12 Applications slots
- Up to 200 W/module at 45ºC ambient, 2.8KW Shelf
- Redundant speed controlled DC fans



Mezzanine Card Option 3x7inch Hot Swappable Up to 8/Mbrd



Advanced Telecom Computing Architecture

- How it gets A= Five 9's
  - Standard hardware, shelf manager, software
  - Redundant Controls Backbone of Controllers, Serial links
    - Any controller or link can fail without failing modules in Shelf.
  - Dual independent 48VDC power conditioners to each slot
    - All modules keep operating of one feed fails
  - All serial multiple dual Gigabit serial links, TR chip sets
    - Dual star or mesh crate networks customer choice
  - On-Board Smarts: Dual Standard Shelf Manager:
    - Controls temperature by fan speed, compensates for failed fan, sees standard chip monitoring circuits in every module, detects failed module and powers down for technician "hot swap", returns module to service after replace, smooth power ramp to eliminate inrush transients, informs processors to reroute data around failed channel, communicates with central management system.

Systems That Never Shut Down

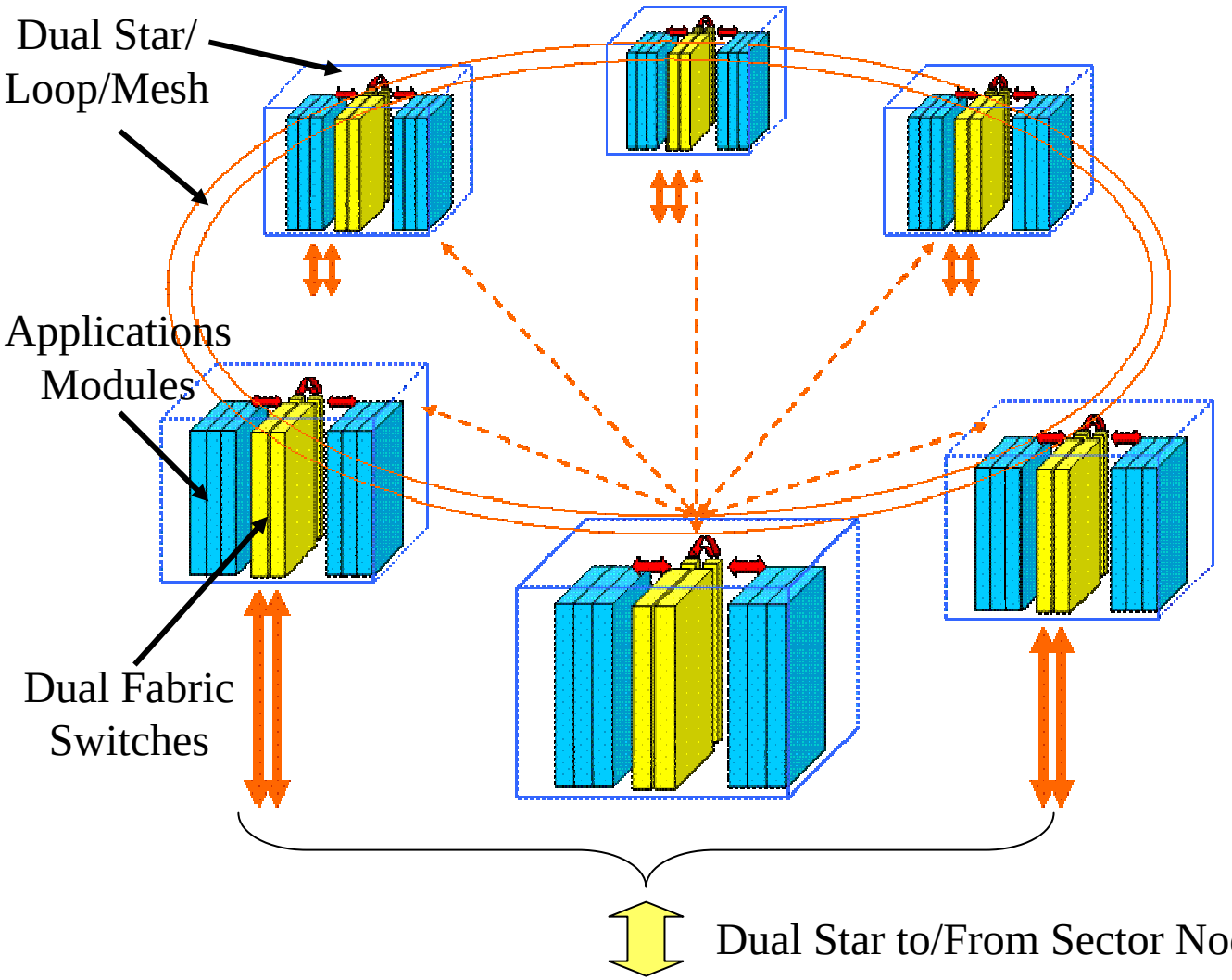
- Any large telecom system will have a few redundant Shelves, so loss of a whole unit does not bring down system – like RF system in the Linac.
  - Load auto-rerouted to hot spare, again like Linac.
- *Key: All equipment always accessible for hot swap.*
- Other Features:
  - Open System Non-Proprietary – very important for non-Telecom customers like ILC.
  - Developed by industry consortium[1] of major companies sharing in $100B market.
  - 20X larger market than any of old standards including VME leads to competitive prices.

[1] *PICMG -- PCI Industrial Computer Manufacturer's Group*

III. How Applicable to ILC Systems?

- ATCA shelf has 14 modules, 2 dedicated to backbone, so 12 application modules about size of large VME but dual wide 1.2in. What might this do?
  - Each of 12 modules can carry up to 8-25W hot-swappable mezzanine cards, or 96 in a shelf.
  - Each mezzanine card could carry 1 or 2 RF or BPM channels. A double height unit could hold a corrector power supply, tuner motor driver or vacuum pump driver, perhaps an SC Quad supply.
  - Redundant power and communications backbone, 2-level hot swap capability is excellent match to many critical front end instruments.
  - Finally, a single card system is possible where standard shelf results in too long cable runs to critical sensors.

Controls Cluster



FEATURES

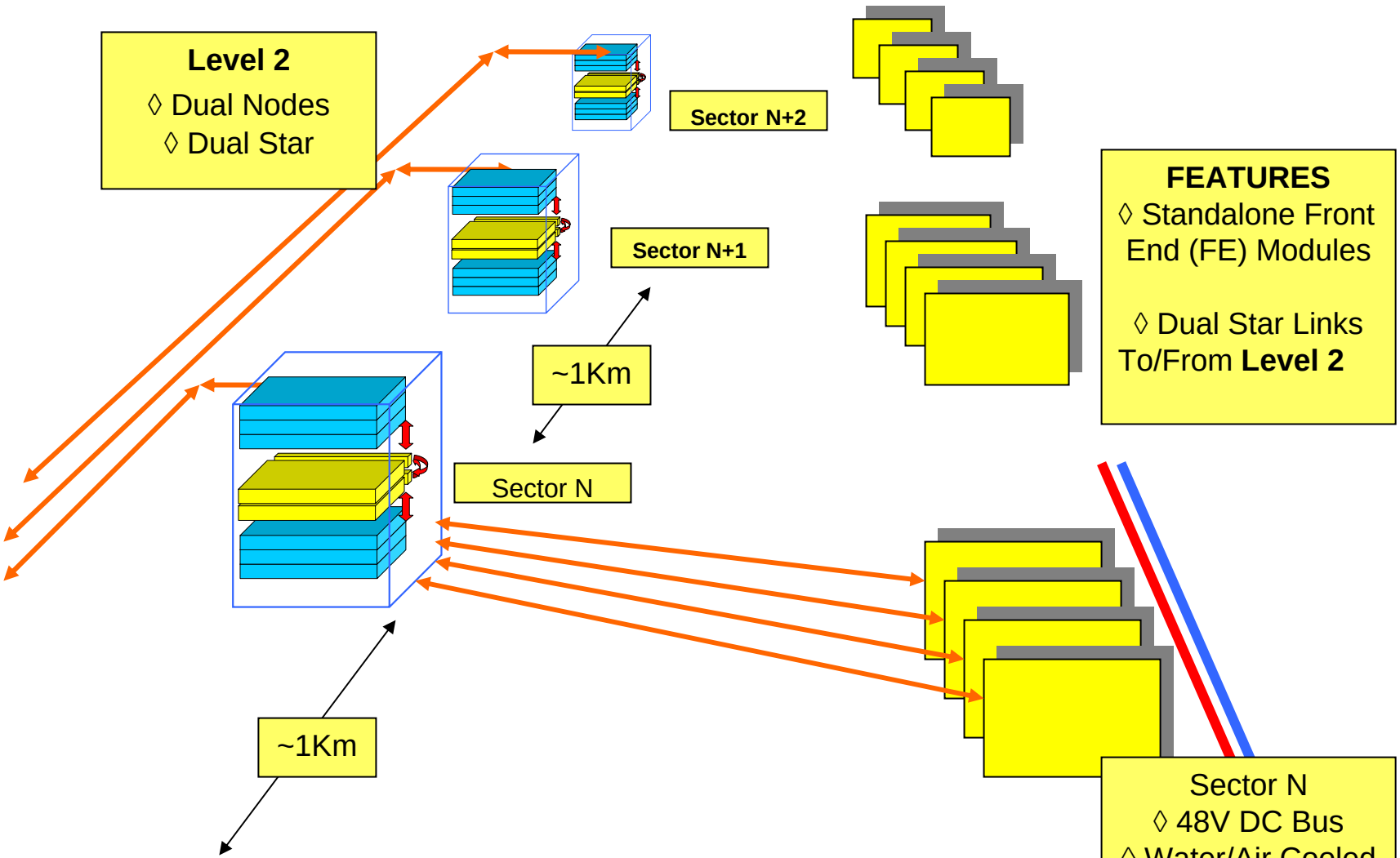
◊ Dual Star 1/N Redundant Backplanes

◊ Redundant Fabric Switches

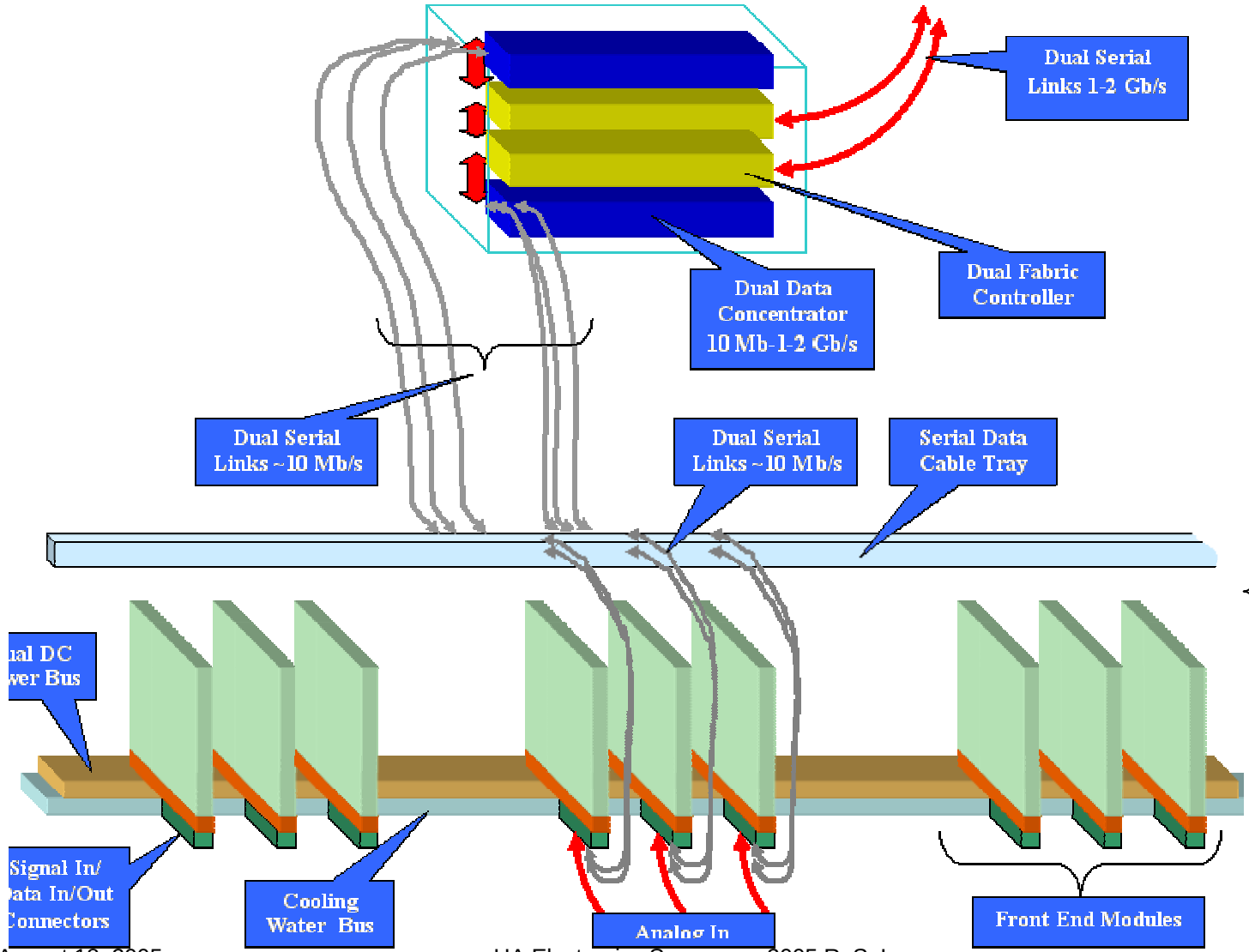
◊ Dual Star/ Loop/ Mesh Serial Links

◊ Dual Star Serial Links To/From **Level 2** Sector Nodes

Sector Nodes

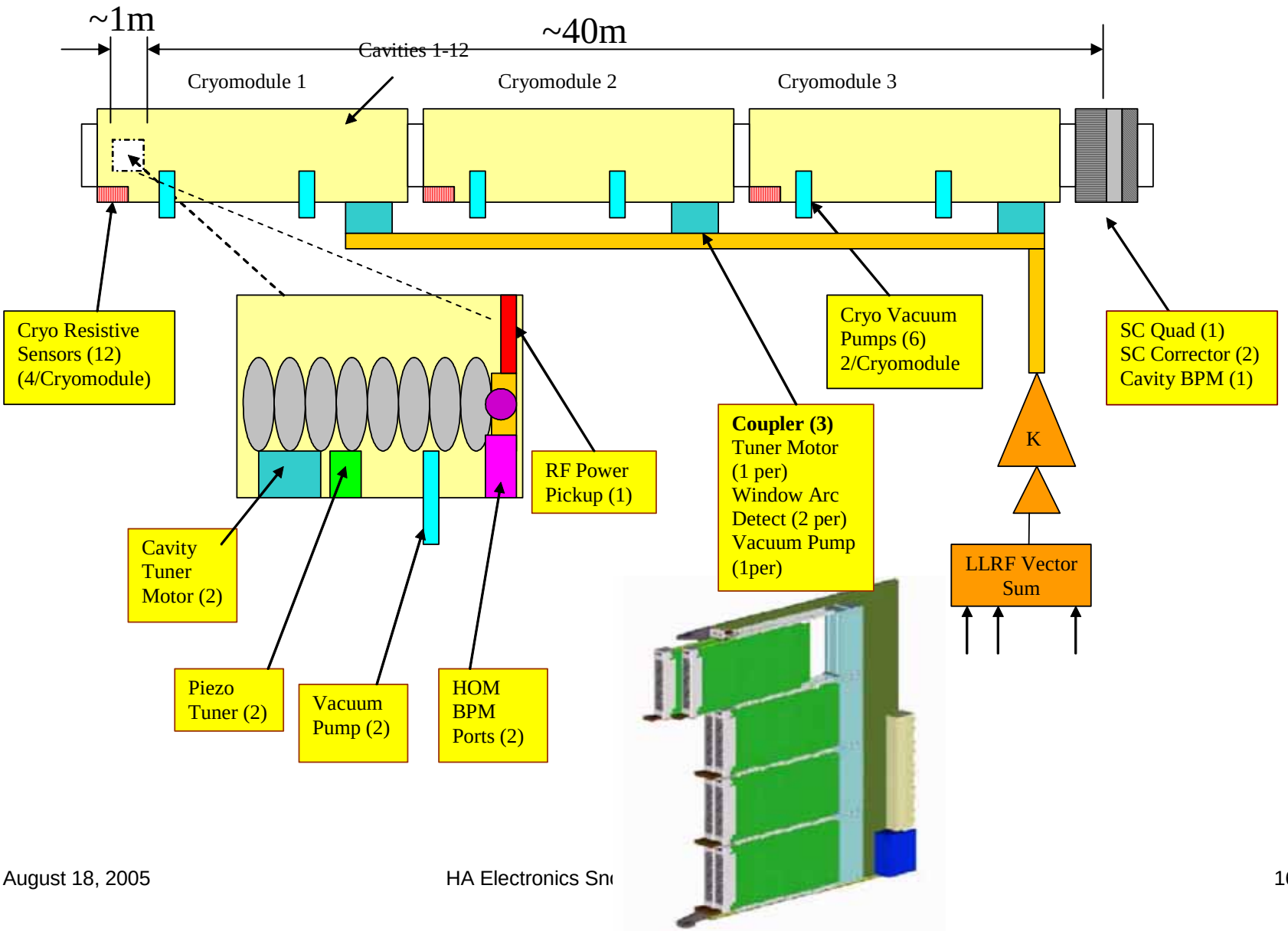


Beam Instrumentation



- ATCA Style Modules
- Stand-Alone or Cluster
- Dual Redundant Serial I/O, Power
- Robotic Replaceable

Front End Instrumentation



ATCA Application in ILC

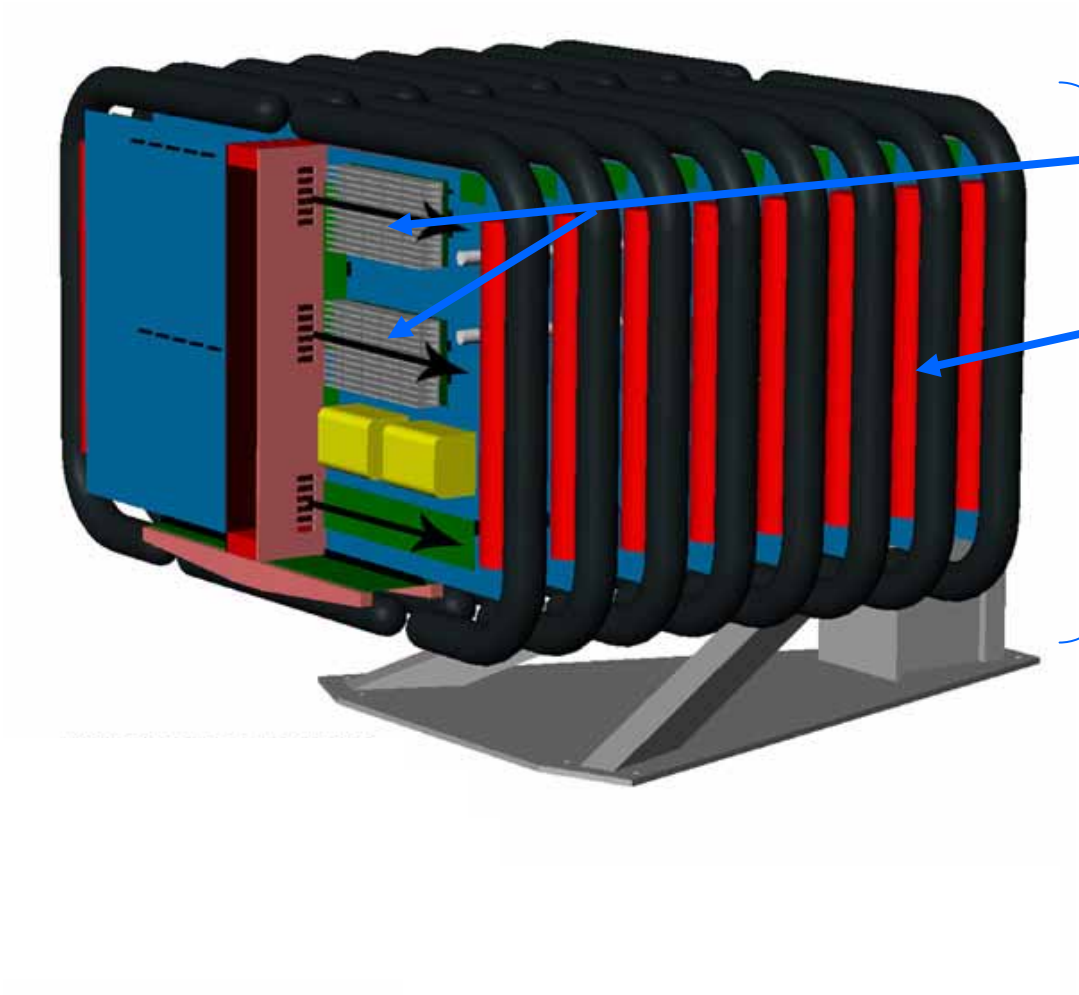
- ATCA Directly Applicable
  - 1. Controls, Networks & Timing
    - Central Control Cluster, IOC's, Sector nodes, Dual Star Networks
  - 2. Beam Instrumentation
    - LLRF, Cavity Tuners, BPM's, Movers, Temp., Vacuum
- ATCA Principles Applicable
  - 3. Power Electronics
    - Modulators, Large Bulk Power Supplies, Modular Power Supplies, Kickers
  - 4. Detectors
    - Power systems, data communications chipsets, protocols, modular packaging, front end interfacing

Review of Design Principles

- HA Design principles are simple:
  - Must not allow a single point failure of one electronic element to bring down machine
  - To achieve must include modest level of *redundancy* at one or more levels:
    - 1. Subsystem level, e.g. a few extra controls crates (units) in the main computer farm
    - 2. Subunit level, e.g. a few extra processor modules within the main computer farm crates
    - Sub-unit level, e.g. hot-swappable daughter cards on a critical PSC module in the beam instrumentation complex.
    - Must have access for hot swap – by worker or machine.
  - Degree of redundancy, hot-swappable implementation depends on element's criticality of interrupting machine.

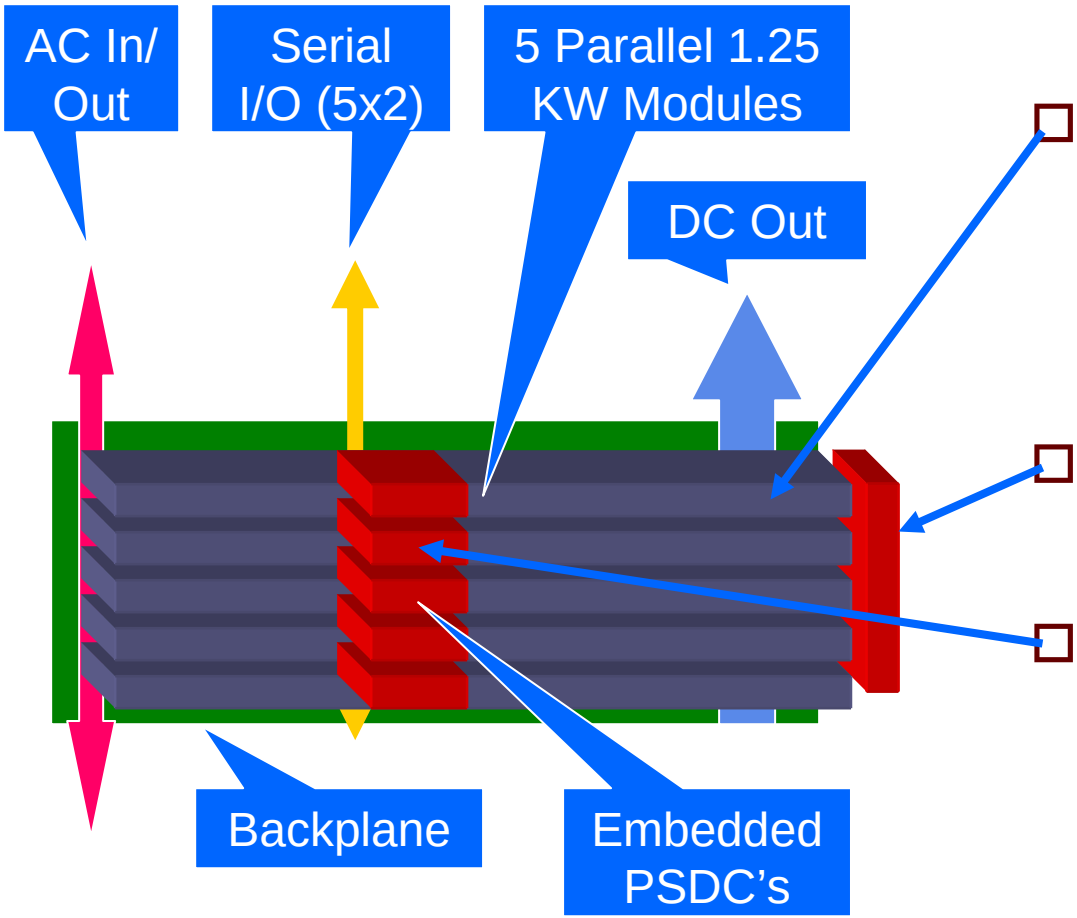
Example Applications of Principles to Other ILC Subsystems

HA Concept Modulator



- 3-Level n/N Redundancy
  - 1/5 IGBT subassemblies
  - 1/8 Mother-boards
  - +2% Units in overall system
- Intelligent Diagnostics
  - Imbedded wireless in every MBrd
  - Networked by dual fiber to Main Control

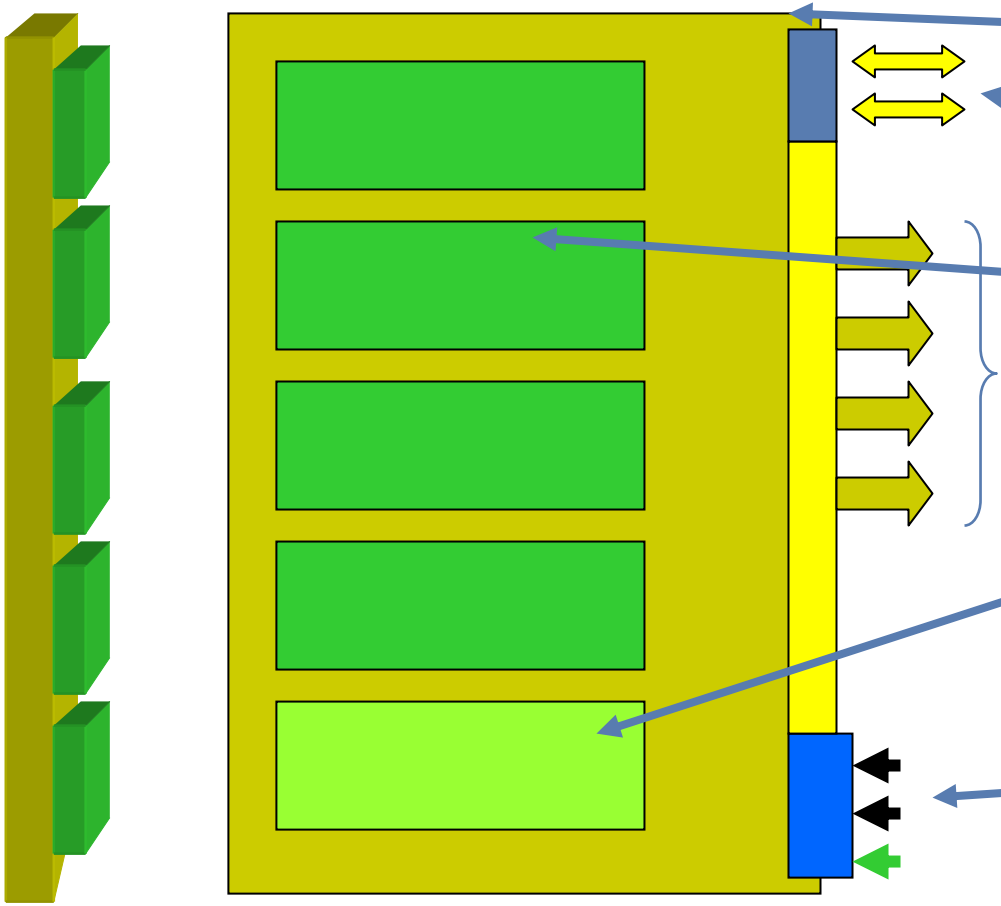
HA Concept DC Power



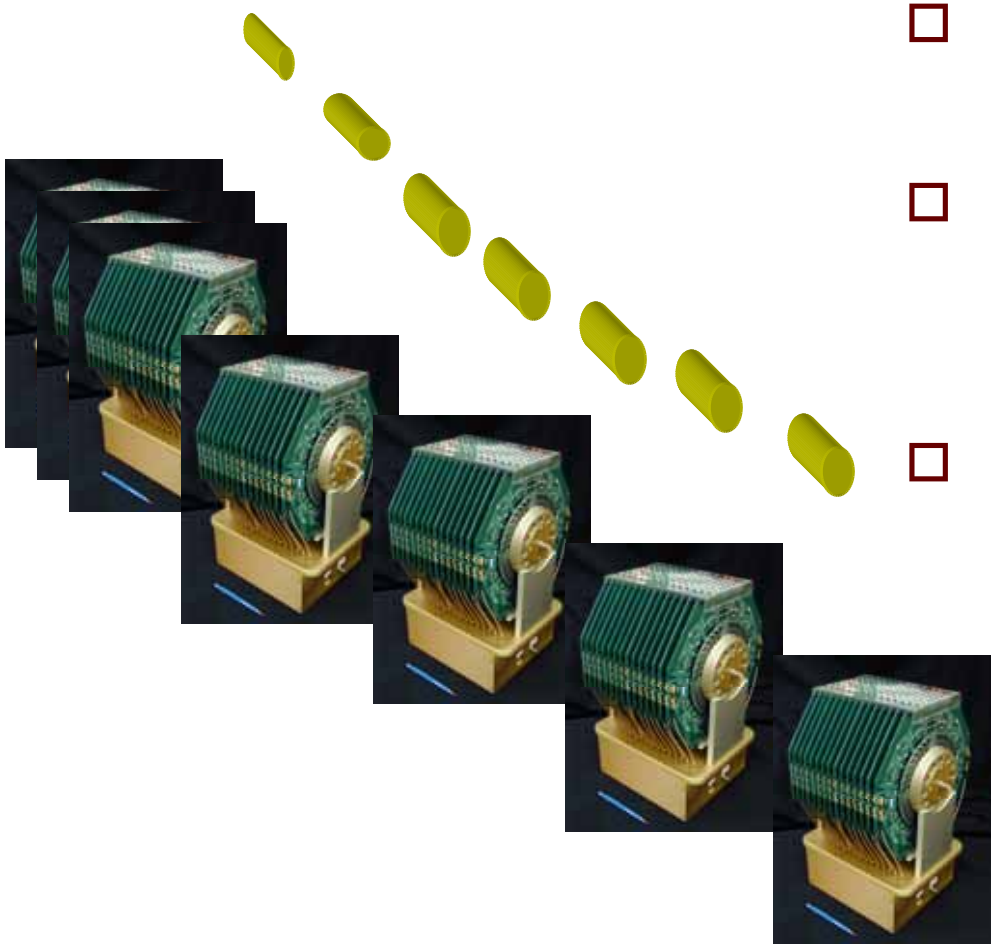
- n/N parallel modules for DC magnet supply (1/5 shown)
- Overall load current feedback
- Independent dual Diagnostics Controller Mezzanine Card each module

HA Concept DC PS Module

- Features
  - Motherboard
  - Dual Serial Control IO
  - Independent Carriers Hot Swappable
  - Optional: Redundant n/N w/ Switchover
  - Dual Bulk 48V DC In



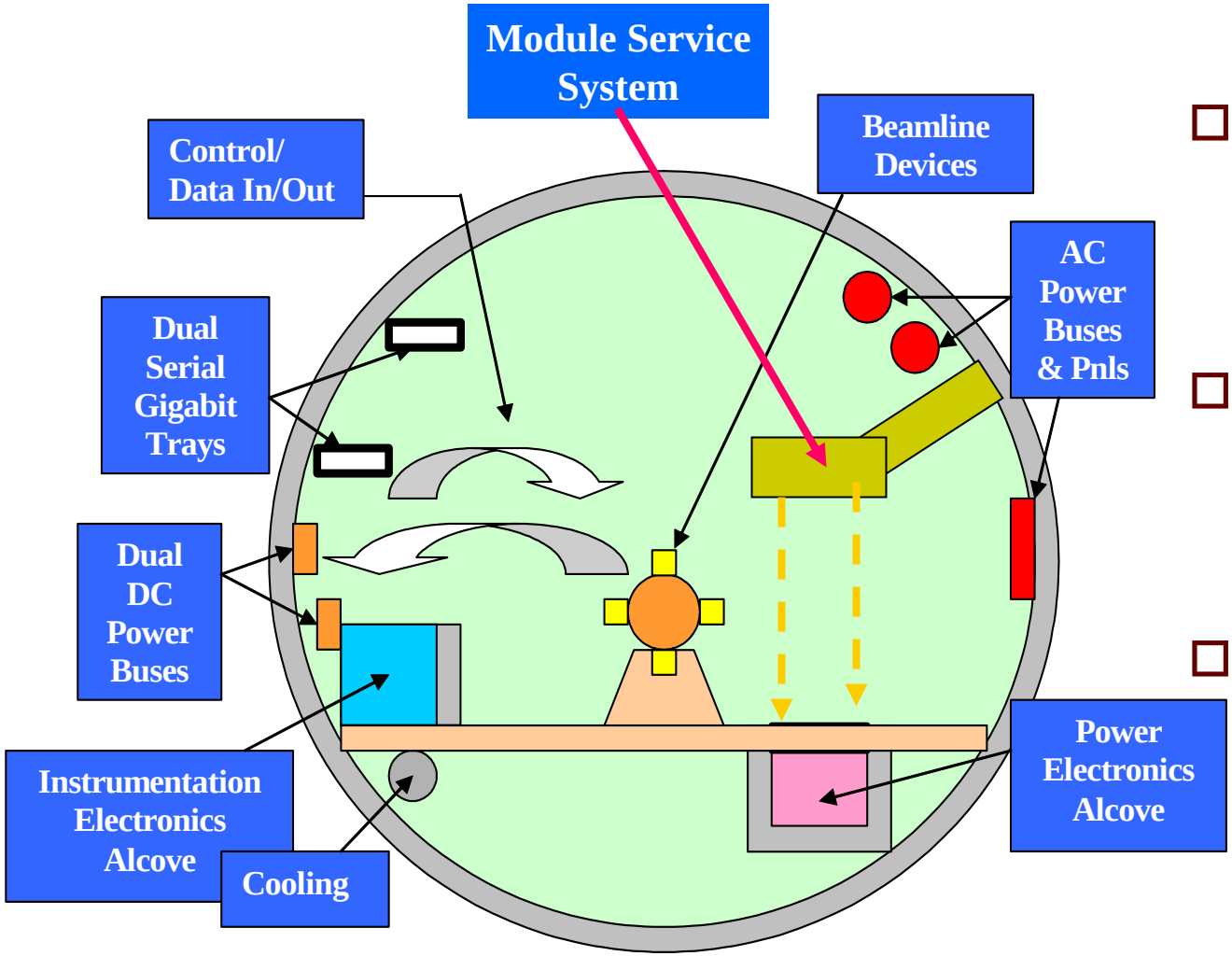
HA Concept DR Kicker Systems



- Approx 50 unit drivers
- n/N Redundancy System level (extra kickers)
- n/N Redundancy Unit level (extra cards)

Diagnostics on each card, networked, local wireless

HA Remote Servicing Concept



- Module replace while operating
- Depot maintenance system
- Instrument & Power Modules

IV: Need for Standards

- Our old, noble instrument standards are far too obsolete to support the powerful new IC technologies of today. Parallel backplane crates are obsolescent; serial wire, fiber and wireless has taken over. *The old ways will not work for ILC!*
- ILC needs to adopt packaging standards within which all the custom creative design work will fit. ATCA is the best and newest instrument system available, *the only open HA system*; it will last for the life of the project.
- Custom adaptations must be made in the power and detector fields where form factors must be flexible, but design principles and Engineering Best Practices will remain firm.
- *It is urgent that ILC evaluate and adapt standards in these early years so platforms are firmly in place when engineering design begins in earnest.*

V. Recommendations

- ILC Electronics controls and instrumentation systems should modernize on ATCA type High Availability platform, readily adaptable to emerging technologies.
- ILC custom Systems design should include ATCA features including equivalent of Shelf Manager.
- In Power Systems such as Marx and LGPS design new *diagnostic layer* to pinpoint problem areas to:
  - *Avert* impending failures
  - Call attention to *treat* failures promptly *without machine interruption*
- Apply to other large units, e.g. Detectors, that don't fit ATCA form factor by adopting concepts and scaling design features.

VI. Conclusions

- Electronic subsystems can attain amazingly high Availability with conscious design of units and subunits to avoid single failure interruption.
- Typical 1/n redundancy in power units, n~5, plus either or both extra units at subsystem level and extra subunits at the unit level. The new Marx design is an example.
- With these measures and access to swap, most system failures can be averted.
- Higher MTBF is always desirable but is not a substitute for HA design.
- MTTR can never be zero but failures that would normally interrupt machine can be avoided by hot-swapping in a 1/n subsystem unit design.
- We should challenge every subsystem, starting with electronics, to strive for HA design. Our goal should be a machine that *never* – well, hardly ever -- breaks .