ISBN: 978-3-95450-132-8 doi:10.18429/JACoW-IPAC2014-THPRO115

CONTROL SYSTEM DESIGN CONSIDERATIONS FOR MYRRHA ADS

R. Modic, G. Pajor, K. Zagar, Cosylab, d.d., Ljubljana, Slovenia
D. Vandeplassche, L. Medeiros Romão, R. Salemme, SCK•CEN, Mol, Belgium

Abstract

The accelerator is the first step of the accelerator driven system (ADS). A high power continuous wave accelerator is required for ADS applications. An essential aspect of accelerator for ADS is beam availability. It must be an order of magnitude better than current best systems. High availability may be achieved by fault tolerance and redundancy of the accelerator. Three factors play a key role here: use of components in a high MTBF regime, parallel and serial redundancy of components, ability to repair failing elements. In terms of accelerator controls system (CS) EPICS and Linux is chosen as proven technology. High availability will be achieved through making parts of the CS redundant. Subsystems shall be redundant by design. If failure of a subsystem is detected, pre-defined scenarios should kick-in. System model or "virtual accelerator" can be implemented to predict effects of parameter change, determine required configuration of set points for optimal performance or re-configuration in case of sub-system failure. Implementation of predictive diagnostics can harvest large amount of data created by archiving service. Prediction of failure allows for controlled shutdown as opposed to abrupt stop.

ADS

MYRRHA is a research reactor conceived as an Accelerator Driven System (ADS) and constituted by a subcritical core fed by an external neutron source. This source is obtained by spallation reaction through a high power proton accelerator, a superconducting LINAC, accelerating a high current proton beam up to 600 MeV. The MYRRHA project [1] aims to demonstrate the feasibility of the ADS concept and the operability of a safe and efficient long-lived radioactive waste transmuter, and moreover, to establish a multipurpose and flexible irradiation facility based on a fast neutron source.

The most significant accelerator design requirements [2] include the Continuous Wave (CW) delivery of a high power beam accompanied to an outstanding design specification of 250 hours as Mean Time Between Failures (MTBF) - being a failure a beam trip longer than 3 s - corresponding to less than 10 failures over a 3 month operation cycle.

The allowed beam trip frequency is significantly lower than observed on today's state-of-the-art comparable accelerators [3], therefore the issue of reliability is considered the main design challenge. Fault tolerance capability is addressed by design, implementing redundancy in both parallel and series manners: the parallel scenario is mandatory in the injector, while the serial scheme (replacing a missing element's functionality by retuning adjacent elements with equivalent functionalities) can be accomplished where high degree of modularity of the accelerating and focusing structures is present (main superconducting accelerator section). Reliability is increased with exploitation of components far from their performance limits, with adoption of reliable diagnostics and powerful and fast controls for fault detection and quick machine reconfiguration. Provisions for online repairability and short Mean Time to Repair (MTTR) are required to guarantee high system availability.

CS

A general-purpose control system is computer-based, hence consists of software and hardware. In the case of MYRRHA, special attention needs to be given to reliability.

Architecture

General guideline for architecture is to standardize and define control system interfaces for all delivered components and devices ideally at the time of procurement. Considerable focus is directed into scalable design. Interoperability and maintenance must be taken into consideration. Typical 3-tier architecture is foreseen, each tier accents different performance features [4].

Software Platform

The need for real-time performance of Input/output controller (IOC) operating system is unlikely since most real time feedback loops will be developed below the level of the IOC. The operating system should have configuration management mechanisms that support software installation, upgrades, and maintenance from a centralized location. CODAC is considered as central CS. Selection of Linux OS seems to best address various performance requirements and can provide suitable front ends and user interfaces. The EPICS framework is widely used as the control system infrastructure for large scientific installations [5]. The power of EPICS lies in its ability to allow communication between large numbers of networked computers to provide control and receive feedback about the numerous distributed parts. The key concept of EPICS is a process variable (PV) which represents a physical quantity that is measured by a sensor or controlled by an actuator. PVs are identified by a name, which must have be globally unique name. An important consideration is to introduce a naming convention early in the project.

CS Services

Relational database will be used to store crucial MYRRHA data. Alarm (BEAST) [6], archiving (BEAUTY) services will be set-up. Virtual accelerator

ISBN: 978-3-95450-132-8 doi:10.18429/JACoW-IPAC2014-THPRO115

concept allows to have a simulation of the accelerator running at all times and assist: predict effect of changing a certain set-point, help determine optimal configuration, mitigate faults and help restore the beam, enable development and integration of the control system before the start of commissioning making it smoother.

Use of predictive diagnostics based on achieved data to forecast failure enables a controlled shutdown and failover to a more reliable redundant component.

Hardware Platform

A decision on a common hardware platform should include its maturity, performance, use in other facilities, obsolesce management. Highly-mature platform such as cPCI is suitable for applications with not so strict performance requirements.

Even choosing a mature platform, one of the biggest development cost drivers are the development and QA of device drivers. It is advised that MYRHHA joins efforts with other similar facilities currently in development and chooses the same platform. This way, development and QA costs and risks can be reduced/shared.

Availability

The impact of high availability requirements on the control system architecture is twofold.

Firstly, the control system itself must not be a bottleneck to high availability. Since the control system is a critical part of the overall system, its complete malfunction would result in malfunction of the facility. Thus, the control system should have high availability, e.g., by making the parts of the control system infrastructure redundant. Technical means of achieving this are discussed in the following subsections.

Secondly, the control system must facilitate other subsystems to achieve high availability. For example, when a failure of a subsystem is detected, a redundant reserve scenario should kick in. The responsibility to coordinate activation of such a reserve scenario is of the control system. Since, in case of MYRRHA, the fail-over time is quite short (3 seconds), the control system must allow for a quick response. If it is not feasible to compute and apply a reserve scenario in an ad hoc manner, the reserve scenarios must be pre-computed and distributed to all nodes, and then just signalled to quickly come into effect. This is the e.g. responsibility of the control system's timing system.

IOC Redundancy

Redundant IOC implementation is not included in the mainline EPICS base [7], and thus not officially supported by the EPICS maintainers. However, since EPICS version 3.14.10, hooks have been placed within the EPICS base that allow implementation of a redundancy scheme [8].

Example redundant IOC architecture is shown in the Figure 1.

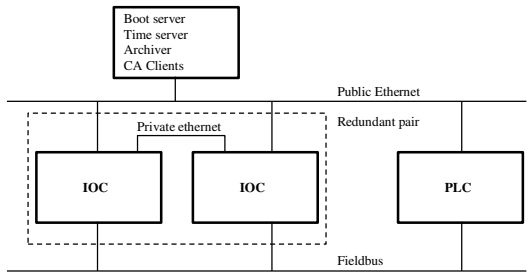

Figure 1: Example of redundant IOC scheme.

In this scheme, each IOC in the pair of redundant IOCs has a connection to the other IOC of the pair through which a heartbeat message is periodically exchanged. One of the IOCs is a primary, and one is a backup. The primary takes on the role of a usual IOC, i.e. it responds to Channel Access requests, and connects to underlying equipment. The back-up, on the other hand, does not respond to Channel Access requests, nor is it connected to the equipment. However, the primary IOC sends all state changes (e.g., changes of PV values) to the backup, which maintains its own copy of the state that is thus always kept in sync.

In the absence of the heartbeat message, the backup node assumes that the primary has failed and takes over, in the same state where the primary left off.

PLC Redundancy

Programmable logic controllers (PLCs) are widely used in industry where high-availability is a frequent requirement. This is particularly the case for safety-critical applications such as medical devices and nuclear installations, where the use of PLCs is also commonplace.

PLCs achieve high-availability through redundancy. Depending on the model of the PLC, the redundancy can be achieved by installing a second CPU. Care must be taken that the same software is installed on both PLCs.

The same applies for I/O and communication modules, which can also be installed in pairs to provided redundancy.

PLC module bus usually has support for hot-replacement of modules. Thus, a failing module can be replaced without needing to shut-down the system.

Network Redundancy

Standard network topology is a multi-level star topology. At the core of the star are backbone switches, to which edge switches are connected. Computer nodes are connected to the edge switches.

In such topology, a failure of a switch, or a cable connecting switches, results in loss of communication for many nodes. Failure of a node's network interface or cable connecting the node to the switch results in loss of communication just for that node.

To mitigate this effect, switches of critical parts of the network should be redundant, as shown in Figure 2. Furthermore, critical computer nodes should either have

ISBN: 978-3-95450-132-8 doi:10.18429/JACoW-IPAC2014-THPRO115

two independent network interfaces, or be fully redundant.

The Ethernet and Internet Protocols which are the basis for all control system communication are designed to recover from a fault in the network in a robust way. However, the recovery is not immediate and may interfere with the real-time requirements of the MYRRHA accelerator control system. Since recovery may take up to several seconds, this could interfere with the MYRRHA's ability to recover a beam within 3 seconds.

Techniques to recover from a network fault quickly exist and include:

- Predefining routing tables on nodes and switches so that backup routes are found more quickly.
- Maintaining and communicating over redundant connections between nodes such that their paths do not share switches or links.

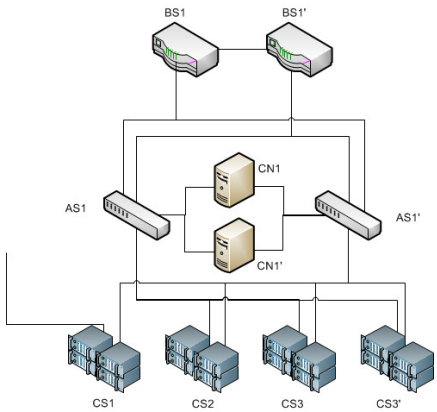

Figure 2: Redundant network topology.

ROADMAP AND PERSPECTIVES

Design of accelerators for ADS applications has reached a mature level for practical implementation, with well identified technological solutions where the current challenge is set all around the reliability issue. EPICS is a proven control system where provisions for high availability can be achieved. Hardware redundancy may be foreseen making parts of the CS redundant. Software implementation of failure prevention and mitigation can be achieved via reserve scenarios and system modelling.

MYRRHA currently entered the Front-End Engineering Design (FEED) phase and is expected to be operational at full power by 2025. In 2013, an accelerator injector test-stand has started being developed within SCK•CEN in collaboration with LPSC Grenoble [9]. EPICS 3-tier architecture is being developed as control system with adoption of cPCI IOCs along with Linux. Micro Research Finland (MRF) timing transport layer based on FPGA has been chosen as reference for the timing system. Industry-based field bus (Profibus) and automation (PLC) solutions are retained as applicable for device integration. This small-scale prototype will serve as the proof of concept for technologies to be used later with the full-size ADS, providing feedback and eventually a complete package of consolidated solutions for the final accelerator implementation.

REFERENCES

[1] A. Aït Abderrahim, "MYRRHA an Innovative and Unique Research Facility", AccApp'11, Knoxville (2011), p. 1.
[2] D. Vandeplassche et al., "The MYRRHA Linear Accelerator", WEPS090, IPAC'11, p. 2718.
[3] J. Galambos et al., "Commissioning Strategies, Operations and Performance, Beam Loss Management, Activation, Machine Protection", Hadron Beams 2008, Nashville, Tennessee, CPL04, (2008), p. 489.
[4] Paul D. Sheriff, "Fundamentals of N-tier Architecture", Barnes & Noble, (2006).
[5] EPICS Home Page, Argonne National Laboratory: http://epics.aps.anl.gov/epics/index.php
[6] Kay Kasemir, "BEAST – Best Ever Alarm System": http://ics-web.sns.ornl.gov/css/docs/BEAST.doc
[7] J.L. Dalesio, L.R. Dalesio, "IOC Redundancy Design Doc", internal report, (2005).
[8] K. Furukawa, "Redundant IOC", EPICS Meeting, (2009).
[9] R. Salemme et al., "The R&D@UCL program in support of the MYRRHA Linear Accelerator", TC-ADS2, (2013).