WHAT IT TAKES TO MAKE A SYSTEM RELIABLE

M. Clausen, M. Möller, S. Rettig-Labusga, B. Schoeneburg, DESY, Hamburg, Germany

Abstract

What is a reliable system and how is reliability defined? This depends on the actual situation and in which environment the system is operated. If you can rely on a scheduled downtime of the controlled system every week, reliability is defined in hours or weeks. In this case the system must run just longer than the scheduled downtime. If the system has to continuously operate for months and even years, your requirements are rising. In cases where continuous operations must be guaranteed even during software or hardware updates, redundant systems come into play. The hardware selection process is driven by basic requirements like 'no moving parts' or 'redundant power supplies'. This implies the selection of possible (fan-less) CPU boards with passive cooling. It also implies no hard discs and reduces therefore the selection of possible operating systems. Continuous operation during updates requires redundant controllers/ CPUs also in addition to redundant power supplies. The latter has a lot of impact on the software running inside the controllers. We will describe the selection process of the components we have chosen and summarize our experience of several years of operations.

REQUIREMENTS

The requirements for process controllers in cryogenic systems are extremely high. Cryogenic systems have to run 24/7 in periods lasting for a year or more. A downtime of the control system will typically cause a downtime of the cryogenic plant of two to four hours to recover cryogenic operations. This does not take into account the systems being fed with liquid helium or the accelerator operations depending on the helium supply.

For the new European XFEL the situation will be even more extreme. The cold compressors of the cryogenic plant are extremely sensitive to distortions of any kind. Any unstable environment will cause an immediate shutdown of the cold compressors. The recovery time is expected to be between twelve and twenty hours at least. Stable process controls have an even higher priority.

POSSIBLE APPROACHES

How can these necessary uptimes be achieved? At DESY we have gained a lot of experience with commercial process control systems. They have the advantage to be supported by a company and should expectedly be reliable. The disadvantage being that they provide a closed environment. No ‘special’ functions which are necessary for cryogenic controls can be easily integrated. As an example cryogenic temperatures need dedicated calibration curves of a 5^{th} to 7^{th} grade polynomial. There’s no easy way to these running in a commercial environment. Another example are dependencies on the operating system, if not on the frontend controllers then at least on the operator screens. Security updates on the Windows operating system may cause problems in the operator’s programs or the commercial software may define the time of system updates or hardware changes while the rest of the Window systems run on a different upgrade pace.

Using PLCs

PLCs may be a solution to reach stability. Predictive continuous processing speeds for all processing blocks in a PLC ensure stability in this respect. Thus PLCs are ideal candidates for machine protection systems. Full process controls on PLCs have certain limitations in processing functionality (see temperature calibration) and transparent data exchange with the operator interface. By default the PLCs do not support transparent data exchange for each and every property of the processing blocks. Each possible connection must be explicitly configured.

Redundancy in PLC controls is partly available but the selection of possible candidates is limited.

Using embedded (real-time) Systems

There is a lot of experience at DESY using embedded real-time systems for process controls. We are using vxWorks on the front end processors and EPICS as the process control system. This combination is typically used for machine controls. At DESY we added and/ or improved the processing block in EPICS to make them process control ready. EPICS comes with transparent access to all properties of the processing blocks. No specific configuration is necessary to gain access to these properties. This is a big advantage over PLCs. On the other hand EPICS did not come with redundancy support.

Redundancy

Redundancy is an important feature when 24/7 operations shall be guaranteed over periods of more than a year. Hardware problems on the processor, on I/O boards or on the control system Ethernet may cause system failures. These hardware problems can be overcome by adding a second processor running the same process database and sequence program in parallel. In case of a failure the second processor will take over without shutting down the controlled cryogenic plant. This kind of redundancy support has been added to the EPICS based control system. This kind of setup shall also help during software updates in the future.

PROCESSORS

We started with VME processors when we started using EPICS at DESY. This was the initial platform for EPICS IOCs. The disadvantage of VME is that a complete VME crate is necessary for a single CPU. And

ISBN 978-3-95450-124-3

this is typical layout of a front-end processor which controls cryogenic components. All of the I/O is connected to field-buses at the beginning CAN and nowadays Profibus (DP). Just one to three field-buses comprise the full I/O system of a major cryogenic plant. A full blown VME system would be overdone. In addition these systems come with active cooling of the power supplies and of the processor boards. This should be avoided. Any moving parts should be removed from a stable long running front-end system.

Compact PCI for Front-End Systems

We have chosen Compact PCI (cPCI) as the backplane bus for the front-end systems. The processor itself should also run without active cooling. It is hard to find low power consumption processors. Low processor speeds are a rare requirement. We have chosen a CPU board from Kontron Company in Germany the CP-305 which comes with enough processing speed and more than enough memory. The power consumption is about 10W total.

No moving parts – no disks

Using vxWorks as the operating system eases the implementation of a diskless front-end. The operating system is downloaded at boot time from the load host. It is memory resident and has only a small footprint. No disk is required to operate such a system.

Power Supplies

Besides the low power processor boards it was difficult to find low power and (of course) redundant power supplies for the cPCI crates. A special design provides good efficiency at low power consumption and can therefore be operated without active cooling.

This way all the necessary components for the cryogenic process controller can be operated fan-less.

LOAD HOST

Because of the diskless character of the front-end controllers it is important to provide a stable and reliable load host. Otherwise the controllers cannot be started since they are diskless. We have installed a redundant system consisting of a two node Sun cluster with a third node as an adjacent test node (Figure 1). Sun clusters are the most reliable cluster setups on the market. Linux clusters cannot compete with them. The most important service on the cluster is the tftp load service. This is also used as a cluster service which causes a failover if it or the cluster node fails.

Disk Storage

Initially the storage was connected directly to the cluster nodes. Nowadays it is more convenient to use network attached storage (NAS). This way the cluster node as well as other computer on the control network can access the disks directly. We are currently using a redundant set of Netapp nodes. For now they reside in the same cabinet but it is planned to separate them to increase the availability in case of a major problem in the computer room.

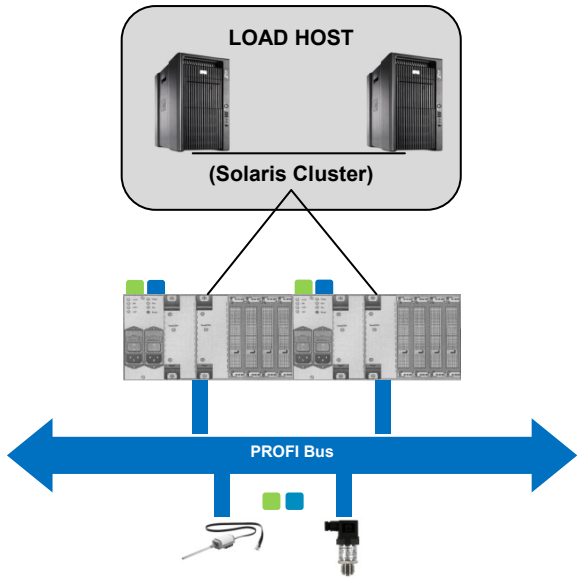

Figure 1: Redundant IOCs connected to a redundant load host.

The same kind of separation can also be applied to the Sun cluster. Availability and reliability are trade off of cluster separation. This is still under negotiation.

NETWORK

The controls network is directly connected to the global DESY network. The main difference being that the connection is not implemented on layer two but on layer three the - routing layer. This way any kind of

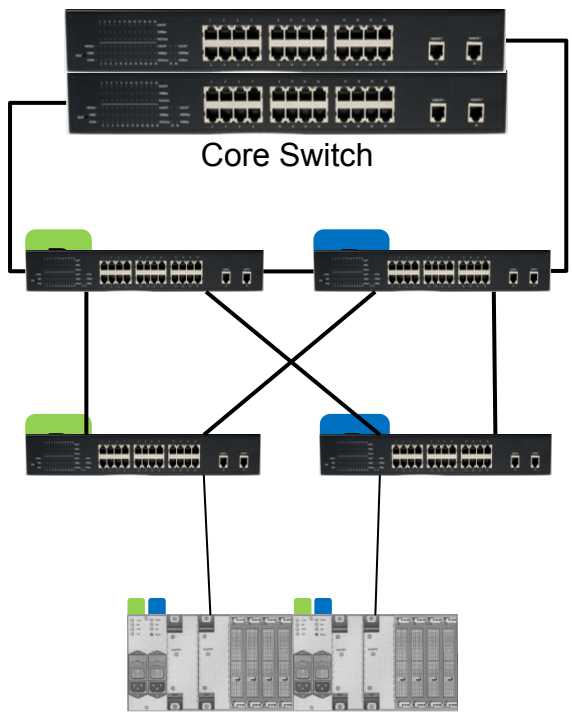

Figure 2: Redundant Network - Redundant Power (A | B).

ISBN 978-3-95450-124-3

management traffic of the routers cannot propagate into the controls network. Any connection between switches or routers in the network is redundant (Figure 2). Spanning tree helps to organize the proper paths. Redundancy is also implemented on the core switch level. Each building hosting control components is connected by a redundant set of core switches. These are configured in a way that any one of these can fail with seamless takeover by the redundant partner.

POWER

Wherever possible components are equipped with redundant power supplies. This applies for front-end controller, major network components, the Sun cluster and the NAS disks. If redundant power is not feasible then we will make sure that e.g. the network switches for the redundant front-end controllers are connected to different power sources. Power sources are in general battery backup systems which keep up for at least ten minutes. These UPS systems themselves are connected to a reliable main supply. This will be powered by a diesel generator within half a minute after a power fail.

Keeping the control system - including the I/O components - up and running after a power fail has proven to be very useful. This way the operators can still see what's going on in the process when the power is down. Especially when pressure rises or valves are open (which should not) it is useful for the operators to get support from the control system.

SUMMARY

Over the course of more than twenty years we have gained experience how to set up control systems for cryogenic plants. Redundancy is mandatory in many areas. Beginning with redundant UPS systems and ending at the redundant temperature sensor. We even developed a package ourselves to support redundancy in the EPICS toolkit. So far our experience with this setup is very positive.

ISBN 978-3-95450-124-3