High Availability for the Price of a Spare

New HA technologies make implementing redundancy strategies for PLCs/PACs and edge controllers easy and more economical.

As the demand in industry for more uptime and efficiency becomes greater, the need for high availability (HA) technology and systems that assure continuous operation likewise increases. What once might have been considered an acceptable lapse in operations – the time to install a spare part, for example – is often today far too great a risk in an industrial application. Key examples are industrial automation controllers.

Democratization of Redundancy

Large scale distributed control systems (DCS) have had HA functions built in for a long time because major process plants, such as oil refineries, are dependent upon them. But for machine and equipment programmable logic controller (PLC) applications, the practice is rarer and typically applied to only the most critical applications and system functions. The reasons are various. PLC/PACs and edge controllers are highly reliable and, in practice, seldom fail. PLC-based systems are generally highly disparate and often proprietary. The processes for building in redundancy in a PLC or edge controller have frequently been complex and costly. Therefore, a cost/benefit analysis made a simple spare part backup the most cost-effective approach to a controller failure.

Figure 1: A small fire in the control room of a cruise ship damaged the controller resulting in loss of control of the ship, requiring it to be towed to port with passengers aboard.

Now, however, PLC/PACs and edge controllers play an increasingly critical role in most industrial applications, including key functions in data analysis and communications. At one time, having a controller fail might have taken a single machine offline. Today, it can significantly impact uptime and efficiency. While failures may be infrequent, any possibility greater than zero can be unacceptable. For example, a cruise ship at sea had a relatively minor fire in the engineering control room that resulted in damage to the control system and a total loss of control of the ship including power, propulsion, ballast management, water treatment, HVAC and more, requiring that the ship be towed to port with paying customers on board. This failure could have been avoided with the correct redundant control system installation in place.

New Methods to Extend Redundancy

The best news, however, is that modern PLC and controller technology, such as that from Emerson, makes it possible to implement HA in these systems easily, rapidly and at a cost little greater than a spare part. It is simple and cost-effective to assure that edge control technology is available without interruption. In this white paper, the methods for easy implementation of HA in edge controller technology are discussed.

This new HA approach using controller redundancy offers three key advantages that underpin a “smart plant” strategy: HA increases uptime, mitigates risk, and supports stronger cybersecurity.

Designers and engineers will naturally explore many considerations surrounding the value proposition of implementing HA, such as:

- Cost: Is additional HA equipment and installation worth the price?
- Space: Will HA equipment fit in the typically constrained available space?
- Training: What degree of additional training will be needed for personnel to support HA solutions?
- Complexity: What amount of labor is necessary to develop, deploy, manage, and maintain HA solutions?
- Failure modes: What deterministic system failure modes could still be possible with certain HA implementations, and how can these be mitigated?
- Geo-redundancy: What is involved to ensure an HA solution is resilient to localized catastrophes?
- Cybersecurity: How do HA solutions support control system software patching without introducing downtime?

Let’s look at how HA redundancy works and addresses all these issues.

Adding a Second Controller

Modern PLC/PACs and edge controllers, such as the Emerson PACSystems™ RX3i controller, provide a solution so two controllers can support the same system, running in parallel, fully synchronized, and locked together in real time with access to the same I/O. This way, the controller ceases to be a single point of failure since a fault in the primary controller can cause a transfer to the secondary in a matter of milliseconds. Emerson accomplishes this through a patented reflective memory technology, which completely transfers an image of the necessary memory from a primary (active) to a secondary (standby/backup) controller every single scan.

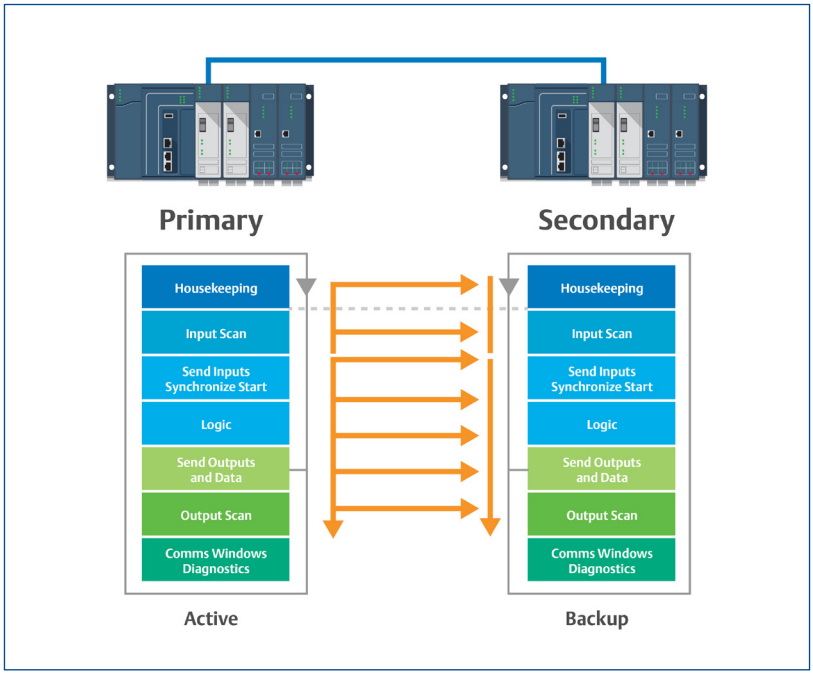

Figure 2: Reflective memory allows a primary controller to mirror to a secondary in real time, down to each individual scan. This allows failover in the shortest possible time.

How HA is Achieved

Supporting HA requires a range of capabilities and conditions

First, both controllers need the same access to all I/O and field devices, which is best achieved via a fault-tolerant Ethernet ring network (Figure 3). Many times, an I/O ring can be installed with not much more materials and effort than a linear network.

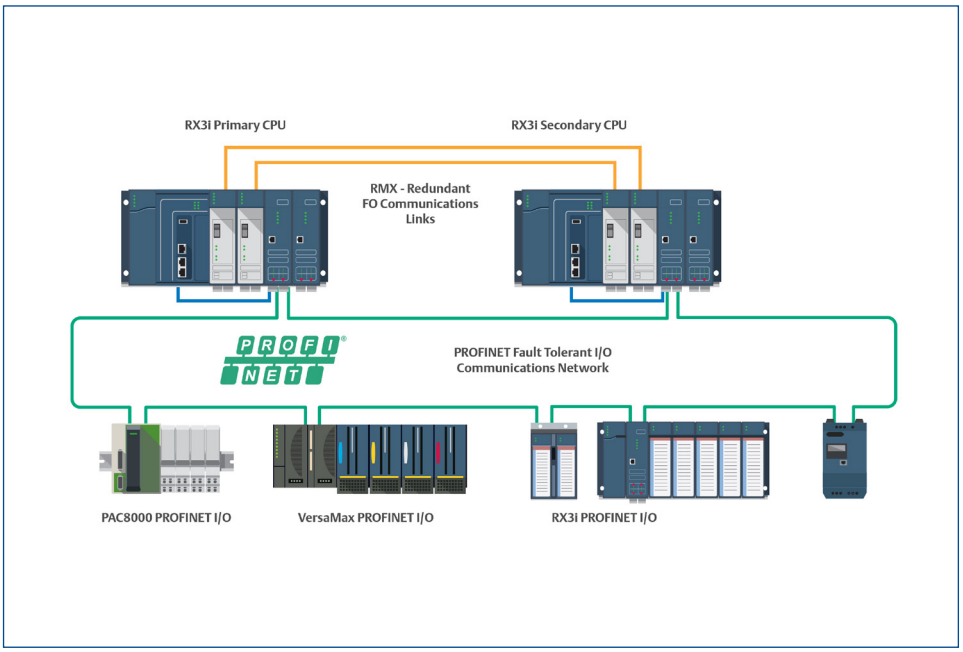

Figure 3: A fault-tolerant PROFINET ring network allows both controllers to be in independent communication with all field I/O.

Second, the two controllers communicate with each other over dedicated links designed to support lock-step synchronization, scan for scan, so the backup always has the same dataset as the primary. This can permit failovers in a single PLC scan, as fast as 5 milliseconds depending on the configuration, but the main consideration is that the failover time is deterministic and not variable due to other conditions. Older methods that try to synchronize the two controllers via the I/O networks result in a lag, and usually create a longer 'blind time' where supervisory systems can't access the controller during a failover. In fact, the non-deterministic failover of these older methods can cascade into additional system failures.

Third, while the two controllers can be in the same location, it is best to separate them geographically to avoid both being subject to common localized problems, such as power outages, fire, or flood. Emerson solutions use dedicated controller-to-controller links and supporting I/O networks, and can span distances up to 10 km through the use of fiber-optics (Figure 4).

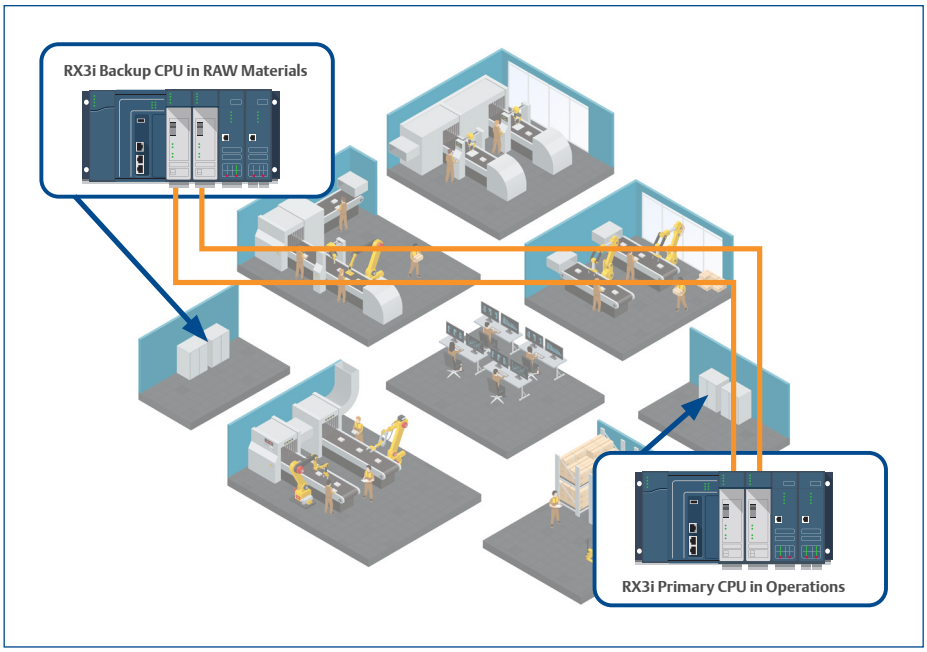

Figure 4: Placing the redundant controllers in geographically disparate locations protects against common-source failures such as power outages and fires.

Fourth, unlike competitive HA redundancy solutions that require their two controllers to be the same hardware model and have identical software and firmware loads, Emerson HA solutions are designed to continue seamless operations even with different software or firmware versions installed on the paired controllers. If the control software or firmware must be updated to deploy a new cybersecurity patch, the primary can be updated while the secondary runs and vice versa. Therefore, the machine or process doesn't need to be shut down as this critical cybersecurity work is performed.

The ability to update the control firmware, software, and even hardware—while the application continues production—can have additional economic benefits for users. Users may now be able to perform routine maintenance and even upgrade activities while the application continues to operate. Activities that were once relegated to night and weekend shifts, meaning costly overtime, can now be readily performed during daylight shifts without sacrificing production. These benefits may help steer users that traditionally did not believe their applications could benefit from HA redundancy to reconsider the benefits of reduced overtime costs and happier maintenance staff.

Another important concern when considering HA redundancy for an application is support for the necessary peripheral equipment to provide a complete solution. Modern I/O architectures using industrial Ethernet protocols, like PROFINET, benefit from having intelligent managed switches to increase the reach and flexibility of control networks. Ethernet switches, especially managed switches, require complex configuration and real-time monitoring to ensure the health of the control network. Fortunately, Emerson's PROFINET-enabled industrial Ethernet switches feature configuration via PROFINET GSDML file, just like standard remote I/O, and the added benefit of an integrated PROFINET I/O Device with PROFINET System Redundancy (PNSR) support. This combination means that these Emerson switches can be configured in PAC Machine Edition, programmed over the PROFINET I/O network, and monitored in real-time from Emerson HA redundant controllers, just like standard PROFINET remote I/O. This capability brings IT capabilities into the grasp of standard OT personnel.

Much like the Emerson PROFINET switches, Emerson's PACMotion VFDs are also designed to thrive in HA redundancy applications right out of the box. The PACMotion VFDs support PROFINET System Redundancy through an optional communications card. When deployed with PNSR support, users can directly connect PACMotion VFDs to Emerson HA controllers, all while maintaining continuous control during controller switchovers and without the added cost and complexity of an intermediary controller to relay data and commands to and from the HA redundant controllers. Emerson's unique set of capabilities and architectures for VFDs can reduce the cost of integrating VFDs with HA redundant controllers by up to 15% while providing improved control and drive oversight.

Emerson makes all these redundancy fundamentals possible without the need to restrict large blocks of memory or sacrifice overall performance. Nor is it necessary to select a controller with more capacity and sophistication than the application requires simply to get one capable of HA. Emerson provides options.

Choosing the Most Economical Approach

Every automation application is different, so it is critical to match controller capabilities to the demands. Some applications call for high control logic performance to manage motion control or high-speed functions. Others need extensive connectivity to higher-level systems and networks.

Emerson offers two families of PLC and edge controller solutions to meet a wide range of needs. Both support open-standard PROFINET fault tolerant I/O ring communication networks to ensure reliable availability of I/O nodes necessary to facilitate HA. Both also make the conversion from simplex control to true redundancy as simple as a few clicks within the configuration software. Users only need to learn one software toolchain, and because Emerson controllers use one runtime the same program can execute in any controller in either simplex or redundant control architectures.

PACSystems RX3i CPE330 PLC/PACs are available in a backplane/rack form factor, providing flexibility and scalability (Figure 5). They provide ultrafast synchronization, with bumpless failovers in a single PLC scan – typically between 5 and 20 milliseconds – while the standalone PACSystems RX3i CPE400 and CPL410 edge controllers deliver 300 millisecond failovers. Configuration is easy, with just a few checkbox selections required.

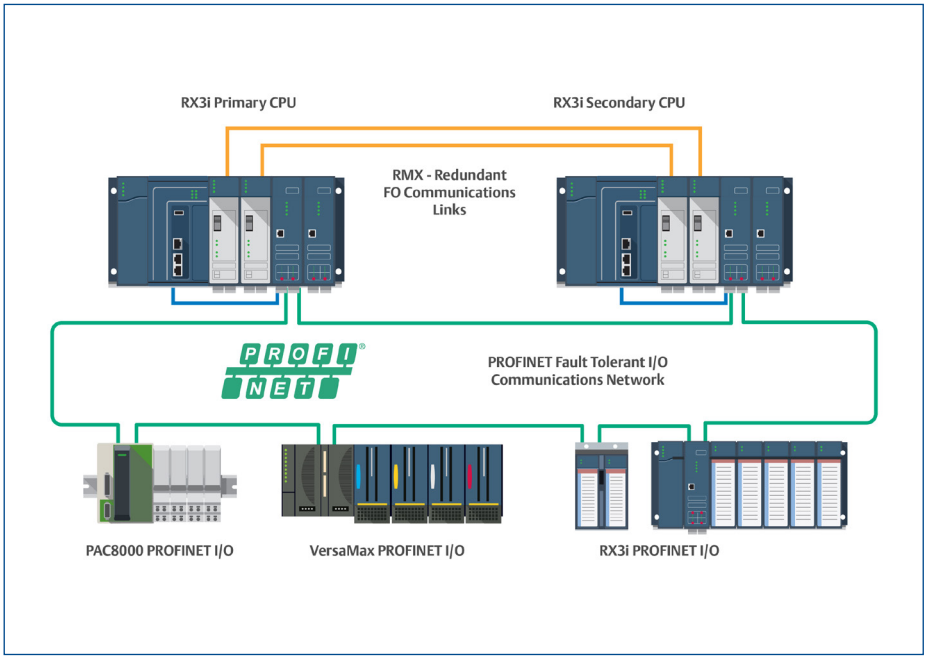

Figure 5: Typical PACSystems RX3i CPE330 PLC/PAC architecture.

The PACSystems RX3i CPE330 is the right choice if the application requires:

- Fast controller failovers
- Additional communication or local I/O modules
- CPUs to be installed more than 100 m apart
- More than 32 redundantly controlled PROFINET I/O devices

PACSystems RX3i CPE400/CPL410 edge controllers are available in a compact standalone form factor (Figure 6). They provide automatic synchronization link recovery, with failovers within 300 milliseconds. Configuration is once again easy, with just a few checkbox selections required.

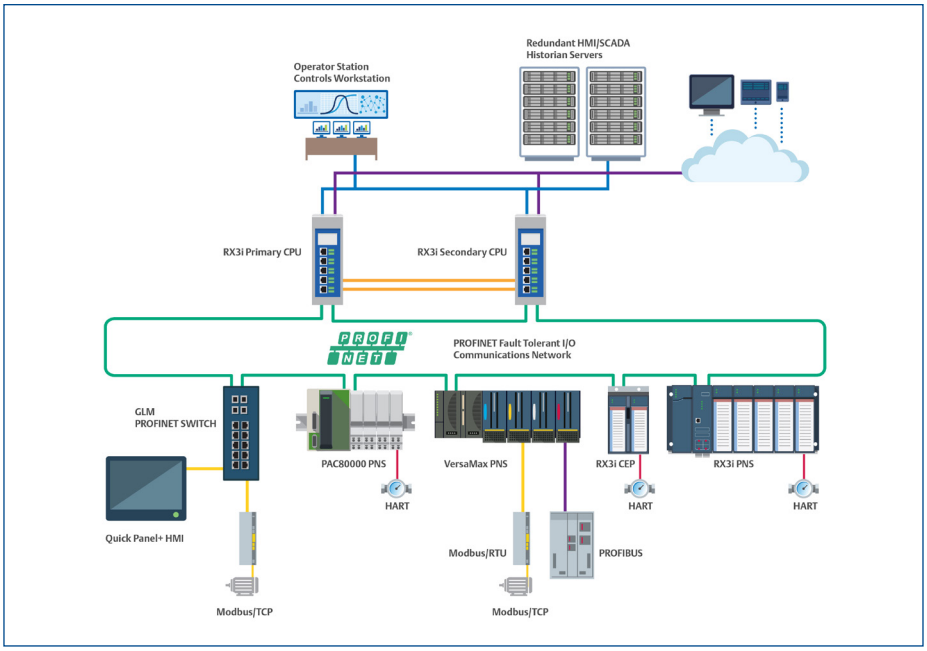

Figure 6: Typical PACSystems RX3i CPE400/CPL410 edge controller architecture.

The PACSystems RX3i CPE400/CPL410 controller is the right choice for less elaborate and lower-budget projects. Still, it can handle critical application requirements, including:

- Quick failovers with no process interruption
- Compact physical footprint, able to withstand -40° to 70°C environments
- Edge application and communication functionality

With PACSystems RX3i controller, PROFINET MRP provides a fault-tolerant I/O network with the addition of just one cable to complete the ring. All I/O solutions offer built-in Ethernet switches. PACSystems RX3i controllers work seamlessly with PACSystems human-machine interface (HMI) and Movicon supervisory control and data acquisition (SCADA) products, and they provide redundant internet protocol (IP) addresses shared between HA redundant controllers to allow simple, seamless communications even with non-redundancy enabled clients and devices.

Choosing a Failover Strategy

The discussion so far has concentrated on hot standby strategies, where both controllers are running and fully synchronized continuously. Some users feel their application may not need this level of protection and choose a less intensive solution.

For example, a cold standby means the secondary unit must be installed in the event of a failure. Obviously, the process must be able to tolerate an outage for at least a few minutes and probably much longer. A warm standby means the secondary controller is powered on and monitoring the primary unit, but some user interaction is needed to restore application control and operation so again there may be an outage for some length of time.

The inferior cold and warm standby strategies are holdovers from earlier, more cumbersome systems and really are not necessary today. With Emerson equipment, there are no longer any disadvantages in operating industrial controllers in a hot standby HA configuration.

High Availability for the Price of a Spare

White Paper
00870-0100-0101
March 2022

HA for the Price of a Spare

A properly configured redundancy strategy ensures an automated machine or system operates with HA. Today, Emerson offers solutions that are easy to implement and priced economically enough to deliver good value. Users don't have to sacrifice top performance related to determinism, diversity, manageability, and security in order to gain HA. When users understand the details behind a world-class redundancy scheme, they can choose cost-effective HA solutions with fast, consistent, and reliable failover.

Contact Us
www.emerson.com/contactus