



Six Steps for Reducing Downtime in Process Automation Applications

EXECUTIVE SUMMARY

Process automation applications are essential to maintaining the operating efficiency, availability and safety of essential processes in manufacturing, pharmaceuticals, oil & gas, power generation and delivery, and other industries. These automation systems provide real-time monitoring and control of complex systems, adding a human management interface and the ability to spot and respond to problems immediately.

Processing automation systems are so valuable in part because they help keep critical processes running and available, and production schedules on target. The potential cost of downtime can be enormous, with analyst estimates ranging from \$44,000 per hour to as high as \$1.6 million per hour for some manufacturing businesses.

What happens when the process automation software itself experiences problems or downtime? There are two possible consequences: data loss, and loss of monitoring and control. Both can have serious consequences for manufacturers.

Data loss: Loss of data about the process can jeopardize compliance with government regulations. In the pharmaceutical industry, you might have to throw out an entire batch if you cannot document it. And you lose traceability – the ability to trace batches and ingredients for recall purposes.

Loss of monitoring and control: The possibility of defects increases when you cannot immediately react to alarms or events. In some cases, such as monitoring pollutants or pressure in pipes, the loss of monitoring can result in danger to employees and others.

This paper outlines six key steps for maintaining the continuous availability of process automation systems. It then describes how Marathon's everRun[®] software supports the continued and reliable operation of process automation systems by *automating* high availability, protecting Windows Servers applications from downtime and data loss.

The cost of downtime in manufacturing

Gartner estimates that the cost of downtime for manufacturing can be up to \$1.6 million per hour



Six Steps for Reducing Downtime: Process Automation

INTRODUCTION

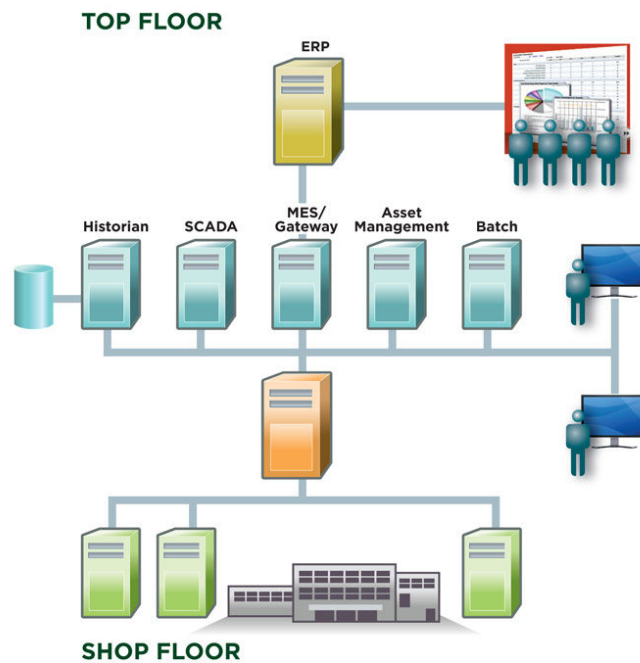
Many things we depend on every day, such as cars, medicine, water, and food, run on systems that may not be completely reliable. However, systems that monitor or control processes, environmental parameters, security or safety, have to be extremely dependable—in fact, they are often required to be close to 100% reliable to prevent any loss of information. These monitoring and control systems, which usually consist of a network of components with a central computer system, are extremely complex and vulnerable to downtime.

Let's look at common examples of monitoring and control systems to understand the impact of downtime on these systems.

PROCESS AUTOMATION SYSTEMS

Process Automation Systems are used by manufacturers in diverse industries such as automotive, pharmaceutical, food and beverage, and energy, as well as water distribution plants. These systems control PLCs, and other intelligent controllers collect data, provide HMI interfaces for operator clients, and provide monitoring and alarming. (See Figure 1 for typical application servers and configurations.)

Figure 1: Process Automation Environment



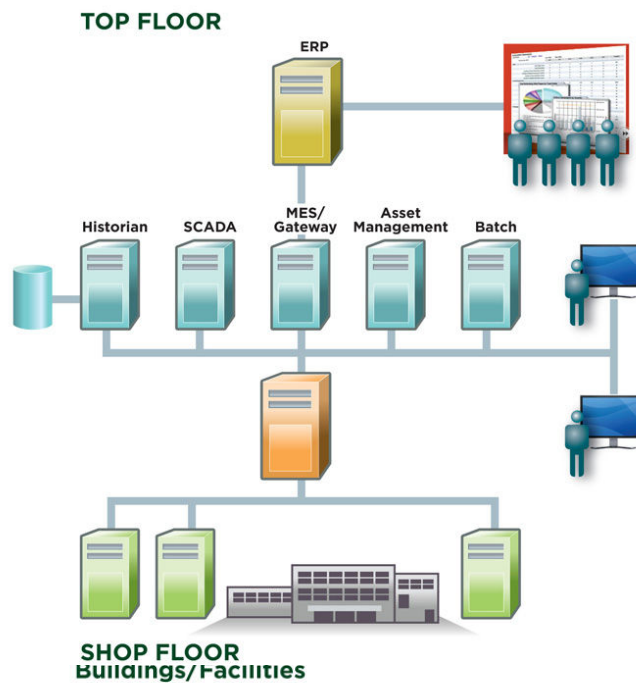


Six Steps for Preventing Downtime: Process Automation

BUILDING AUTOMATION AND SECURITY SYSTEMS

Security systems such as access control systems, video monitoring systems, intrusion detection systems, and others are used in federal buildings, hospitals, large companies, and airports, where devices with data and intelligence are installed all over and networked to a central server providing control, alarming, configuration capabilities, monitoring and reporting capabilities and data logging. (See Figure 2 for typical configurations.)

Figure 2: Building Automation and Security System Environment





Six Steps for Reducing Downtime: Process Automation

SIX STEPS TO REDUCING DOWNTIME

STEP #1: REDUCE HUMAN ERROR

Human error is one of the primary sources of unplanned downtime. There are two main types of human factors that cause or worsen downtime:

1. The initial human errors that cause the downtime
2. Additional errors after an outage has occurred that delay uptime restoration

Niel Nickolaisen, IT process management expert and co-author of the new book *Stand Back and Deliver: Accelerating Business Agility*, says that in his experience working with best practices companies, system downtime can be reduced by at least 70% by defining and implementing a simple IT change management process, which includes identifying and researching the change, performing risk analysis on the change, and consistently communicating the change.

All changes should be reviewed using a cross-functional team, always including the operational people who are responsible for maintaining the changed system. Including a cross-functional review as part of the change management process is essential to avoiding unexpected problems that can lead to unplanned downtime. Different teams may be aware of interdependencies between systems that may otherwise go unnoticed.

For example, when a problem occurs, someone must identify the problem correctly and take steps to address it. To restore service or ensure continued availability, operations teams may need to replace damaged server hardware, restore lost data, replace redundant network connections, and/or reload applications or an operating system.

The next step in reducing human error is to simplify IT processes, including change management processes, wherever possible. As Nickolaisen puts it in his law of inverse entropy: "Left to ourselves, we humans (even IT people) will complicate all processes and guidelines."

To guard against excess complexity, he suggests revisiting and reviewing change management processes regularly, and making changes if:

- Change management processes exceed two pages
- A change review form exceeds one page in length
- A special "emergency" change process emerges because the ordinary

"Left to ourselves, we humans (even IT people) will complicate all processes and guidelines."

- Niel Nickolaisen



Six Steps for Preventing Downtime: Process Automation

process is too time-consuming or complex

The same general principles apply to ordinary operational processes. Managing and maintaining availability in the IT organization should be simple, reducing the strain on expert employees. For example, IT operations staff should be able to:

- Roll back changes easily
- Easily maintain, upgrade or replace an IT infrastructure component without complex processes for switching components in and out of production

Many technologies for high availability actually introduce complexity into the IT environment. For example, clustering technologies may require administrators to painstakingly maintain each server in the cluster to support successful failover.

IT organizations instead should find and embrace those technologies that reduce complexity for operational staff—thereby eliminating potential sources of human error.

STEP #2: REDUCE SERVER FAILURES WITH QUALITY HARDWARE AND COMPONENT REDUNDANCY

Server hardware problems can cause unplanned downtime in several ways:

- Catastrophic server failures caused by memory, processor or motherboard failures
- Failures of server components, including power supplies, fans, internal disks, disk controllers, host bus adapters and network adapters

To reduce the chances of server failures, purchase robust, name brand servers, perform recommended preventative maintenance, and monitor server errors for signs of future problems. Taking these steps should reduce the total cost of operations of your systems.

To reduce downtime caused by server component failures, add redundancy at the component level. Examples include: redundant power and cooling, ECC memory, with the ability to correct single-bit memory errors, and combining Ethernet cards with RAID.

STEP #3: PROTECT AGAINST STORAGE FAILURES WITH STORAGE DEVICE REDUNDANCY AND RAID

With vital real-time data about manufacturing processes, defending against data loss is essential. Use device redundancy combined with RAID storage algorithms to protect data access and data integrity from hardware failures.

For local storage, it is quite easy to add extra disks configured with RAID protection. Use a second disk controller to prevent the controller itself from being a single point of failure.



Six Steps for Reducing Downtime: Process Automation

Access to shared storage relies on either a fibre channel or Ethernet storage network. To assure uninterrupted access to shared storage, these networks must be designed to eliminate all single points of failure. This requires redundancy of network paths, network switches, and network connections to each storage array.

STEP #4: USE REDUNDANT NETWORK PATHS, SWITCHES AND ROUTERS TO PROTECT AGAINST NETWORK FAILURES

The network is another possible source of downtime. The network infrastructure itself must be fault-tolerant, with redundant network paths, switches, routers and other network elements. You can duplicate server connections to eliminate failovers caused by the failure of a single server or network component.

Make sure that the physical network hardware does not share common components. For example, dual-ported network cards share common hardware logic, and a single card failure can disable both ports. For full redundancy, you need either two separate adapters or a built-in network port combined with a separate network adapter.

STEP #5: REPLICATE DATA TO ANOTHER SITE FOR PROTECTION FROM SITE FAILURES

Multiple factors can cause site-wide failures, including an air conditioning failure or leaking roof, a power failure, or a major hurricane affecting a large geographic area. Site disruptions can last anywhere from a few hours to days or even weeks. If your processes must keep running, then you must replicate process automation data to an alternate site to remain operational.

There are two methods for dealing with site disasters. One method is to tightly couple redundant servers across high speed/low latency links, to provide zero data-loss and zero downtime. The other method is to loosely couple redundant servers over medium speed/higher latency/greater distance lines, to provide a disaster recovery (DR) capability where a remote server can be restarted with a copy of the application database missing only the last few updates. In the latter case, asynchronous data replication maintains a backup copy of the database.

Protecting against site failures is an essential part of your disaster recovery planning. Combining data replication with error detection and failover tools to help get a disaster recovery site up and running in minutes or hours, rather than days – reducing any interruption to essential processes.



Six Steps for Preventing Downtime: Process Automation

STEP #6: USE HIGH AVAILABILITY SOFTWARE TO AUTOMATE PROTECTION OF SERVERS, STORAGE AND NETWORKS

Implementing steps 2-5 above requires an investment of time and resources, particularly if you have no automated way to monitor and react to failures in the application infrastructure. Using automated HA software reduces the total cost of operations of your highly available application environment.

Automated high availability software can reduce or entirely eliminate downtime and data loss without adding a lot of overhead. A software solution can monitor and react to failures in systems, storage and networks, automatically reconfiguring resources to enable the application to continue operating with little or no interruption.

The next section of this paper describes everRun®—the automated high availability software developed by Marathon Technologies and its use in protecting process automation systems from downtime and data loss.

EVERRUN® PROTECTS PROCESS AUTOMATION APPLICATIONS FROM DOWNTIME

Unlike cluster or failover solutions that require two fully configured and managed systems, Marathon Technologies' everRun creates a very simple and automated availability solution that requires little setup and configuration while providing the most stable and reliable platform for running all of your critical process automation applications.

The everRun approach to complete application protection includes:

Resilience & Prevention

- Early-warning alerts for preventative management
- Automated I/O redirection in real-time
- Don't wait for failure to happen—prevent it

Real-Time Validation

- Guaranteed failover readiness
- Constant testing & validation of servers, storage & networks

Simplicity & Automated Recovery

- Users are not affected while systems are restored/repaired
- Auto-synching & self-healing
- Low TCO, minimal IT staff requirements, reduced chance for human error





Six Steps for Reducing Downtime: Process Automation

Marathon everRun technology is used by leading automation software vendors including GE, Johnson Controls International, Schneider Electric, Yokogawa, Bosch, Wonderware, Rockwell Automation, Dematic, Siemens and Iconics and others to provide automated availability for their widely-deployed process automation systems. Hundreds of manufacturers around the globe in a wide range of industries rely on Marathon everRun to protect their process automation systems – without IT intervention.

CASE STUDY: SANTA ROSA UTILITIES DEPARTMENT

The City of Santa Rosa, California Utilities Department controls water distribution for approximately 150,000 residents using Wonderware's InTouch™ human-machine interface (HMI) software protected by Marathon's everRun software. Employees optimize system operations by adjusting set-points and monitoring equipment performance, as well as managing time-of-use for pumping schedules to maintain reservoir levels. InTouch HMI software detects pump station/reservoir intrusion and monitors process alarms.

REQUIREMENTS

The Santa Rosa Utilities Department needed a simple, cost-effective way to protect its critical water distribution control system from downtime due to faults, failures and disasters. The protection system needed to eliminate three downtime scenarios:

- Downtime during a water main break, when delayed response could cause interruption of service, flooding, and other costly consequences.
- Interruption of the electricity usage optimization function that saves electric costs by running pumps when electricity is less expensive.
- Downtime during natural disasters. Because Santa Rosa is located in an earthquake-prone area, the control system needs to be protected from earthquake, landslide, and other natural disasters that could interrupt water distribution when it is critically needed.

THE SOLUTION

The City of Santa Rosa chose Marathon's everRun software-based system to meet the City's fault and disaster tolerance requirements. "The Marathon solution was simple, cost effective, and provided a higher level of protection than any other solution we looked at," said Mitch Dobson, Senior Consultant for EMA, the city's control system consulting firm.

WORLDWIDE HEADQUARTERS

Marathon Technologies Corporation
295 Foster Street, Littleton, MA 01460
Tel 1.800.884.6425 / 1.978.489.1100
Fax 1.978.489.1101
Email: info@marathontechnologies.com
Web: www.marathontechnologies.com

EMEA HEADQUARTERS

Marathon Technologies UK Ltd
Regus House, Trinity Court
Wokingham Road, Bracknell
Berkshire, RG42 1PL
Tel +44 (0) 1344.706.241
Fax +44 (0) 1344.706.242
Email: emea@marathontechnologies.com
Web: www.marathontechnologies.com





Six Steps for Preventing Downtime: Process Automation

"The cost savings resulting from this efficient use of staff resources paid for the Marathon software in a short time frame."

John Joyner, City of Santa Rosa

RESULTS

Since the successful completion of the Santa Rosa project, EMA and Marathon continue to work together using Marathon's unique redundant control systems platform at other water and wastewater facilities. "By making our control system continuously available, we can deploy our operations staff to the locations where they are needed around the city," said John Joyner, Senior Manager, City of Santa Rosa. "The cost savings resulting from this efficient use of staff resources paid for the Marathon software in a short time frame."

SUMMARY

Businesses in a wide range of industries rely on process automation software to keep manufacturing processes running smoothly. Using automated HA software helps keep the process automation software itself running smoothly, without interruption.

The six steps outlined in this paper highlight processes and strategies that you can adopt today to reduce the risks of downtime to process automation systems, while containing the cost of IT management. Of these steps, using automated HA software the fastest way to reduce downtime while minimizing administrative overhead.

Marathon everRun is the trusted choice of business around the globe in a wide range of industries with critical application needs. Find out how Marathon can help you maintain and automate availability for process automation systems.

To see everRun in action, watch our product demo videos, or download a free 30-day evaluation license, visit www.marathontechnologies.com

The Marathon logo, SplitSite and everRun are trademarks or registered trademarks of Marathon Technologies Corporation. Microsoft and Windows are registered trademarks of Microsoft Corporation. All other trademarks and registered trademarks are the property of their respective owners. Copyright 2010 Marathon Technologies Corporation. All rights reserved. Marathon Technologies Corporation reserves the right to make changes to this document at any time and without further notice. Marathon Technologies Corporation assumes no responsibility for any errors that may appear in this document.