



Fault Tolerance Redundancy

October 2015
An ICONICS Whitepaper
www.iconics.com



CONTENTS

1	ABOUT THIS DOCUMENT	4
1.1	SCOPE OF THE DOCUMENT	4
1.2	REVISION HISTORY.....	4
1.3	DEFINITIONS.....	4
2	INTRODUCTION	5
2.1	BRIEF HISTORICAL PERSPECTIVE ON HMI REDUNDANCY	5
3	GENESIS32™ REDUNDANCY OPTIONS	6
3.1	ADMINISTRATIVE SERVERS.....	6
3.2	DATAWORX™32 REDUNDANCY	7
4	USING FAULT TOLERANT SERVERS WITH ICONICS PRODUCTS	8
4.1	FAULT TOLERANT SERVERS	8
4.2	FAULT TOLERANT VIRTUAL SERVERS.....	9
4.3	DATAWORX™32/FAULT TOLERANT SERVER COMPARISON	11
4.4	DATAWORX™32/FAULT TOLERANT VIRTUAL SERVER COMPARISON...	12
5	CLUSTERING FOR HMI FAULT TOLERANCE	13
5.1	CLUSTERING HMI	13
6	SUMMARY	14
6.1	GENESIS32™ FAULT TOLERANCE AND REDUNDANCY.....	14
6.2	BIZVIZ™ FAULT TOLERANCE AND REDUNDANCY	15

1 About This Document

1.1 Scope of the Document

This document contains information on the features of several ICONICS products and third party products that may be of use to companies wishing to apply fault tolerance and redundancy to their GENESIS32™ or BizViz™ system. An overview of HMI redundancy schemes and a summary on how they can be applied to the GENESIS32 and BizViz product families is presented.

The intended audience includes engineers working on implementing fault tolerant solutions through redundancy, sales and marketing personnel desiring to gain an understanding of the product features supporting redundancy and end-users looking for information on using GENESIS32 and BizViz in redundant configurations.

1.2 Revision History

Version 8 – Dave Oravetz, John Pettit, Matt Michel, March 16, 2005 (initial release)

Version 9 – Dave Oravetz, July 17, 2005 (V9 update)

1.3 Definitions

The following are acronyms used in this document, and are presented here for reference.

- CPU – Central Processing Unit
- COTS – Commercial Off The Shelf
- FT – Fault Tolerant
- FT Server – Fault Tolerant Server
- FT Virtual Server – Fault Tolerant Virtual Server
- HMI - Human Machine Interface
- I/O – Input / Output
- LAN – Local Area Network
- MSCS – Microsoft Cluster Service
- OPC - OLE for Process Control
- OPC DA – OPC Data Access
- OPC A/E – OPC Alarms and Events
- OTS – Off the Shelf
- SCADA - Supervisory Control and Data Acquisition

2 Introduction

2.1 Brief Historical Perspective on HMI Redundancy

The need for HMI/SCADA fault tolerance and redundancy has been around as long as there has been process control and automation in our factories and facilities. In the early days of instrumentation, HMI fault tolerance was implemented by adding redundant displays or recorders to the critical sensors. This was possible in the days when 4-20ma signals were the de facto industry standard and due to the inherent ability of powered analog signals to drive multiple devices. Given enough space, implementing fault tolerance and redundancy in those days was relatively simple. However, it was far from convenient, and definitely very expensive!

Today, microprocessor-based sensors and high-speed communications networks make it possible to send the signals from thousands of sensors to a single PC workstation or server; functionality that until recently was only possible with expensive DCS systems. Open communications standards such as OPC enable inter-vendor operability, allowing the software running on the workstation to communicate with various types of controllers and a wide range of I/O. HMI/SCADA software solutions like ICONICS GENESIS32™ software make it possible to monitor, control, limit check, data log, replay, and perform a myriad of other functions with this data. As a result, a single PC workstation can now effectively perform the function previously performed by thousands of dedicated HMI display and recording devices.

Reliability and uptime have become critically important because of the mission-critical functionality now concentrated in HMI/SCADA server applications. Improving the reliability and fault tolerance of applications that strictly monitor and view data can be done by simply adding a second or redundant PC workstation. Improving the reliability and fault tolerance for server applications requires strong initial planning. The focus of this paper is the initial planning necessary for high value server application fault tolerance and/or redundancy.

3 GENESIS32™ Redundancy Options

There are several options available for improving the reliability and fault tolerance of the GENESIS32™ and BizViz™ products using ICONICS Redundancy Solutions. The ICONICS product family includes several servers for performing administrative functions (See Section 3.1 for details). These servers are part of the core ICONICS infrastructure and the support for making these servers redundant is included in GENESIS32 and BizViz.

In addition, an optional ICONICS product, DataWorX™32 Professional Edition, can provide support for redundant IO Servers, Alarm Servers, Historical Replay Servers, and provide support for redundant Data Logging capabilities.

3.1 Administrative Servers

The functions of the administrative servers are as follows,

- Security server: a central system security server provides a central repository of all system rights and permissions
- License server: central system product license server
- Language server: provides support for multiple language switching
- Global aliasing server: central file used to resolve aliasing for complete system
- Event server (known as GenEvent server): central log, records all events for the complete system

The ability to designate back-up servers for all the administration servers is a feature of the base product. Both fault tolerant options and both of the redundant design approaches are appropriate for the administration servers.

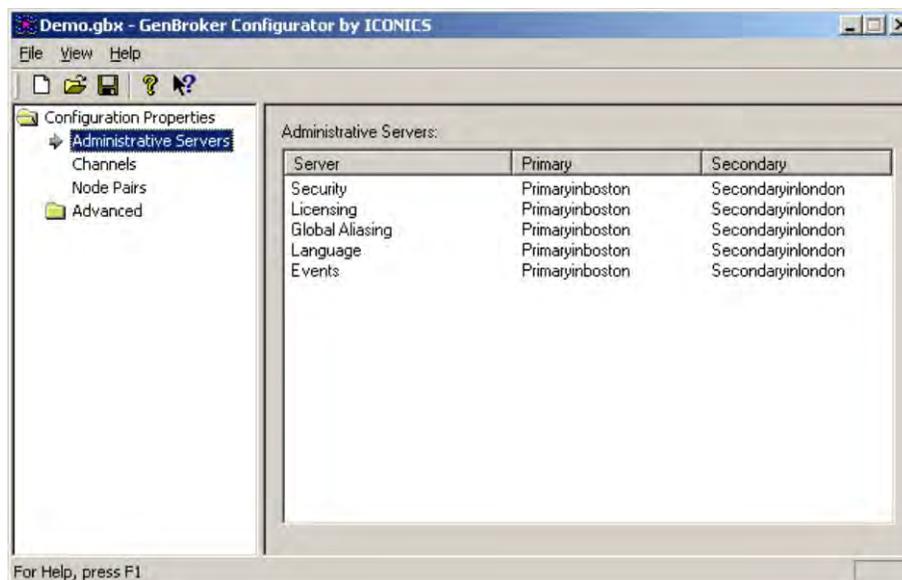


Figure 3.1 – Configuration Screen for setting up Redundant Administrative Servers

3.2 DataWorX™32 Redundancy

The ICONICS DataWorX32 Professional product provides support for redundant IO Servers (OPC DA), redundant Alarm Servers (AlarmWorX32 AE), redundant loggers, and redundant Historical Replay Servers. DataWorX32 is based on a highly integrated approach that is easy to use. Configuring redundancy is very easy as it simply involves entering the node name (or address) of the backup node. Monitoring the status or health of the Primary and Secondary nodes is also simple. The GENESIS32™ built-in MonitorWorX™ function continuously monitors the health of the primary and secondary servers of each redundant server pair and provides bubble popup messages anytime there is a change in status. In addition, built-in process point tags provide status of the redundant pairs and provide the ability to control failovers via logic.

For more information on DataWorX32 Professional and its application, please see the White Paper entitled "DataWorX32 Software Redundancy".

4 Using Fault Tolerant Servers with ICONICS Products

4.1 Fault Tolerant Servers

In addition to using DataWorX32 Professional redundancy support, there are a number of options available for improving the reliability and fault tolerance of the GENESIS32™ and BizViz™ products of ICONICS. One option is to use Fault Tolerant Servers. A Fault Tolerant (FT) server is a “single box” replacement for a Workstation or Server that is designed for 99.999% or greater uptime. Such products typically use replicated, fault-tolerant hardware components and “Lockstep” technology (meaning transactions run concurrently on both halves of the server), so that when a failure does occur there is no downtime or transaction loss. Replicated hardware components typically include the CPU, Memory, Hard drives, and Power Supplies. These systems also include specialized Fault Detection and Isolation hardware and software and so called “hardened” device drivers that are claimed to have higher reliability than the standard drivers provided by Microsoft. The specialized fault detection software not only identifies the failed component(s), but can automatically start the ordering process for replacement parts. Figure 4.1 below shows the architecture for the ftServer W Series Fault Tolerant server by Stratus Technologies, a market leader in the Fault Tolerant server industry

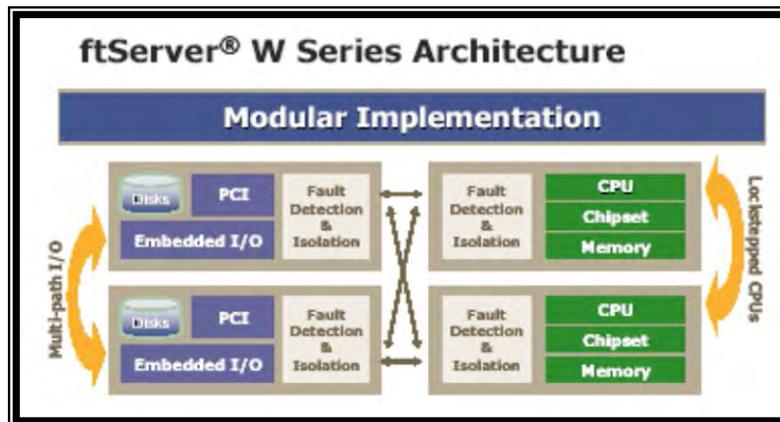


Figure 4.1 – Stratus ftServer W Series Architecture

Stratus Technologies and NEC are two companies that offer FT servers. Both company's products, as one might expect, doubles everything from memory to processors and storage, which allows the servers to keep functioning at optimum levels even when key components break down. This differs substantially from clustering solutions (discussed in Section 5) that depend on a traditional heartbeat link between cluster nodes to initiate the failover process. In the cluster scenario, a secondary server is passive until the primary one fails; it then assumes the responsibilities of the failed server, a process that can take a couple of minutes to finish.

The Stratus ftServer W Series servers are designed for hosting MS Windows based applications and consequently represent the appropriate choice within the Stratus line for PC-based HMIs. One should be aware that most of the 2300's components are NOT hot-swappable, limiting its use to applications that has regularly scheduled downtime. The three other higher-level Stratus models all support hot-swappable

components throughout and are suitable for 24/365 operations. Figure 4.2 shows a summary of the Stratus ftServer W Series products.



Figure 4.2 – Stratus ftServer W Series Product Line

Fault Tolerant servers like the Stratus ftServer W Series servers are compatible with all ICONICS GENESIS32™ and BizViz™ products.

4.2 Fault Tolerant Virtual Servers

A second option available for improving the reliability and fault tolerance for PC-based HMI products and the GENESIS32 and BizViz products is to use Fault Tolerant (FT) Virtual Servers. An FT Virtual server is functionally similar to an FT Server. They both provide redundant replacements for a traditional Server with a targeted goal of 99.999% uptime. The primary difference is in the implementation. Whereas the FT server is a true single box replacement, the FT Virtual Server uses two identical Commercial Off the Shelf (COTS) servers and some special software to replace a single server.

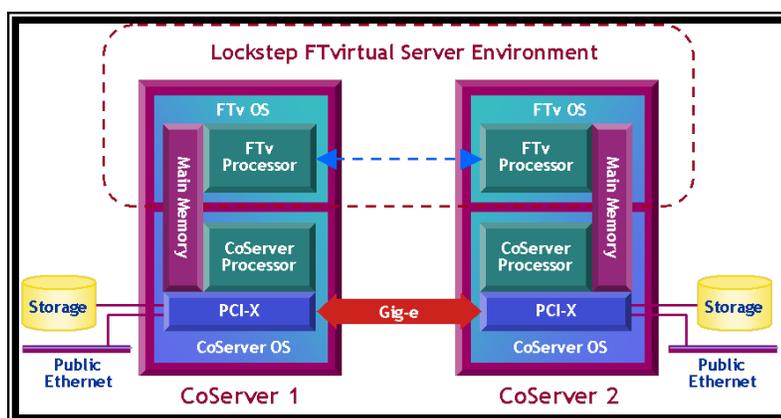


Figure 4.3 above shows the architecture for the FTvirtual Server by Marathon Technologies, a market leader in the FT virtual server industry.

The FT virtual server is designed for hosting Microsoft® Windows®-based applications and consequently, like the FT Server, offers a good fault tolerant option for PC-based HMI's. One feature available with FT Virtual servers that is not available with FT Servers is the option for "Split-Site", which is to separate the redundant servers over a long distance. This feature can provide disaster tolerance. A catastrophic event such as a fire explosion affecting one of the redundant pairs may not affect the backup if the pair is separated by a long enough distance. Figure 4.4 provides a summary of the advantages of the FT Server verses the FT Virtual server.

The minimum configuration for a Marathon FTvirtual server requires two identical servers with hyper-threaded single processors, a pair of Gigabit Ethernet Network Adapters, and the entry-level Marathon software.

Since this article was written, Marathon has replaced the FT Virtual Server product with a similar product named everRun FT. A second product named everRun HA has also been added. EverRun HA's hardware requirements are less strict (you don't need identical machines). However, the everRun HA product doesn't have a "zero" downtime failover, unlike the everRun FT product. Its operation is more like a cluster, where the backup must be started up in the case of a failure of the Primary server.

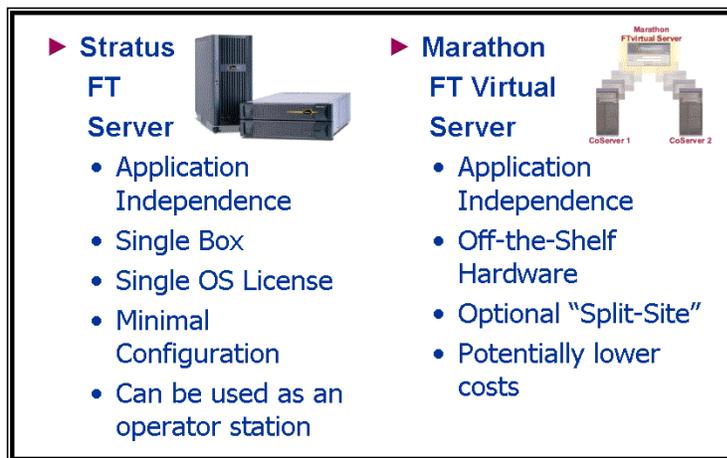


Figure 4.4 – FT Server/FT Virtual Server Comparison

Fault Tolerant virtual servers like Marathon Technologies' FTvirtual server are compatible with nearly all ICONICS GENESIS32 and BizViz products. Exceptions are mainly due to the FTvirtual servers limitation of not supporting the serial, parallel, and USB ports (e.g. support for OPC Servers that communicate using the Serial port, bio-metric software, and hardware key related software are excluded). Running GraphWorX™32 client software or any other GENESIS32 user interface client software on an FTvirtual server is not recommended due to appearance reasons. FTvirtual server duplicates the user interface on both machines and limits the number of screen colors for performance reasons.

4.3 DataWorX™32/Fault Tolerant Server Comparison

DataWorX32 can run on standard COTS (Commercial Off the Shelf) MS Windows workstations and servers. This can provide savings in hardware costs, and savings can be greater for distributed systems with redundant OPC Servers and multiple AlarmWorX32 Servers, systems that could potentially require several FT Servers. DataWorX32 has a built-in Store and Forward capability that enhances the GENESIS32 data and alarm logging capabilities. Should a failure occur in the connection to the database, Store-and-Forward keeps the un-written values in a cache and writes them to the database when the connection is restored. DataWorX32 supports the capability to have the secondary node located at any distance from the primary node. This can provide “Disaster Tolerance”. Upgrading an existing system to DataWorX32 redundancy does not necessarily require replacement of the existing hardware (this depends on the current system being upgraded).

▶ DataWorX32	▶ FT Server
	
<ul style="list-style-type: none">• Potentially lower cost• Scalable Cost-effective Distributed Redundancy• Uses Standard PCs• Store and Forward• Can be added to existing• Remote Secondary node<ul style="list-style-type: none">– Any distance	<ul style="list-style-type: none">• Hardware based• Redundancy is transparent to Application SW• Lower OS SW cost<ul style="list-style-type: none">– Single license• Less configuration• Redundancy Solution for<ul style="list-style-type: none">– WebHMI– BizViz

Figure 4.5 – DataWorX32 / FT Server Comparison

4.4 DataWorX™32/Fault Tolerant Virtual Server Comparison

DataWorX32 runs on standard COTS MS Windows workstations and servers and does not require identically matched server-class machines. DataWorX32 has a built-in Store and Forward capability, which enhances the GENESIS32 data and alarm loggers. Should a failure occur in the connection to the logging database, Store-and-Forward keeps the un-written values in a cache and writes them to the database when the connection is restored. Upgrading an existing system to DataWorX32 redundancy does not necessarily require replacement of the existing hardware (this depends on the current system being upgraded).

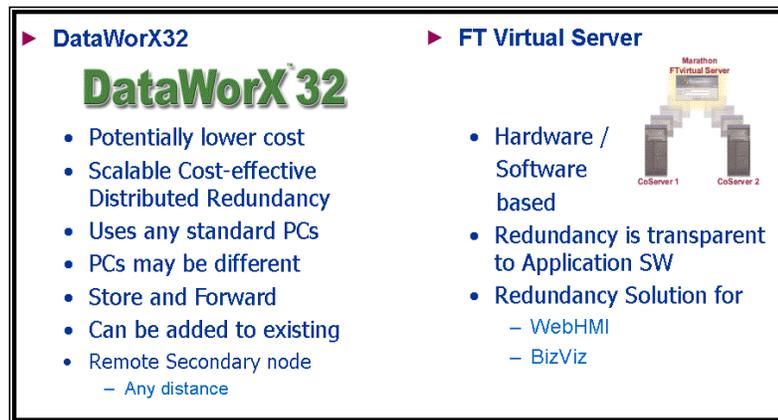


Figure 4.6 – DataWorX32 / FT Virtual Server Comparison

5 Clustering for HMI Fault Tolerance

5.1 Clustering HMI

A third option available for improving the reliability and fault tolerance for PC-based HMI products and the GENESIS32 and BizViz products is to use Clustering. Clustering is a grouping of independent server nodes that are accessed and viewed on the network as a single system. This collection of server nodes makes it possible to provide backup operations where if any resource in the server cluster fails, the cluster as a whole can continue to offer service to users by using a resource on one of the other servers in the cluster, regardless of whether the failed component is a hardware or software resource. In other words, when a resource fails, users connected to the server cluster may experience temporarily degraded performance, but do not completely lose access to the service.

One of the most widely used clustering technologies is Microsoft's Cluster Service (MSCS). This technology supports Fault Tolerance through "Failover". Using Heartbeat technology, MSCS can detect the failure of a cluster-aware application and can automatically restart the failed application on the same node. It can also detect a node failure and automatically move all of the applications previously running on the failed node to another working node. In either case, there will be some downtime for the application, anywhere from a few seconds to several minutes or more, depending on the configuration of the servers and the applications themselves.

While clusters can be designed to handle failure, they are not fault tolerant with regard to user data. The cluster by itself does not guard against loss of a user's work. Typically, the recovery of lost work is handled by the application software; the application software must be designed to recover the user's work, or it must be designed in such a way that the user session state can be maintained in the event of failure.

Any of the ICONICS software applications can be run on a cluster. The time required for a Cluster Service to detect a failed node and to start the applications on a backup server should be taken into consideration. Please contact ICONICS for more detailed information on the use of clusters with your ICONICS applications.

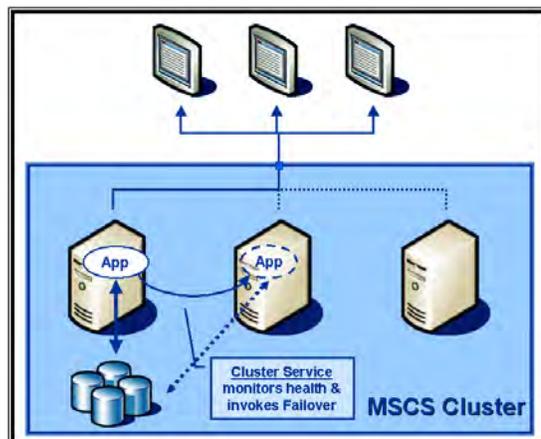


Figure 5.1 – Microsoft Cluster Services

6 Summary

The ability to designate back-up servers for all the administration servers is a feature of the base GENESIS32™ and BizViz™ products.

- **GENESIS-32 Administrative Servers**

 - Security Server
 - License Server
 - Global Aliasing Server
 - Language Aliasing Server
 - GenEvent Server

Figure 6.1 – GENESIS32 Administrative Servers

6.1 GENESIS32™ Fault Tolerance and Redundancy

Figure 6.2 provides the Redundancy options for several of the GENESIS32 modules. The Stratus ftServer and Marathon FTvirtual servers are recommended in nearly every case. One exception is the FTvirtual Server, which does not support serial, parallel, and USB port communications, which could limit its applicability for OPC Servers. DataWorX32 is recommended for OPC Server, Alarm Server and Trend Server Redundancy. The use of clustering depends on the application. Consideration should be given to the cluster's failover time and the application's ability to save its state information through a failover/restart.

ICONICS Product	Stratus FT Server	Marathon FTv & everRun FT Servers	Clusters & Marathon everRun HA Servers	DataWorX 32
OPC DA (Any)	●	○	○	●
AlarmWorX32	●	●	○	●
TrendWorX32	●	●	○	●
ScriptWorX32	●	●	○	NA
WebHMI Server	●	●	○	NA

Recommended
 Application Dependent

Figure 6.2 – GENESIS32 Redundancy Options

6.2 BizViz™ Fault Tolerance and Redundancy

Figure 6.3 provides the Redundancy options for the BizViz products. The Stratus ftServers and Marathon FTvirtual servers are recommended in every case. The use of clustering depends on the application. Consideration should be given to the cluster's failover time and the application's ability to save its state information through a failover/restart.



Founded in 1986, ICONICS is an award-winning independent software developer offering real-time visualization, HMI/SCADA, energy, fault detection, manufacturing intelligence, MES and a suite of analytics solutions for operational excellence. ICONICS solutions are installed in 70% of the Fortune 500 companies around the world, helping customers to be more profitable, agile and efficient, to improve quality and be more sustainable.

ICONICS is leading the way in cloud-based solutions with its HMI/SCADA, analytics, mobile and data historian to help its customers embrace the Internet of Things (IoT). ICONICS products are used in manufacturing, building automation, oil & gas, renewable energy, utilities, water/wastewater, pharmaceuticals, automotive and many other industries. ICONICS' advanced visualization, productivity, and sustainability solutions are built on its flagship products: GENESIS64™ HMI/SCADA, Hyper Historian™ plant historian, AnalytiX® solution suite and MobileHMI™ mobile apps. Delivering information anytime, anywhere, ICONICS' solutions scale from the smallest standalone embedded projects to the largest enterprise applications.

ICONICS promotes an international culture of innovation, creativity and excellence in product design, development, technical support, training, sales and consulting services for end users, systems integrators, OEMs and Channel Partners. ICONICS has over 300,000 applications installed in multiple industries worldwide.

World Headquarters

100 Foxborough Blvd.
Foxborough, MA, USA, 02035
Tel: 508 543 8600
Email: us@iconics.com
Web: www.iconics.com

European Headquarters

Netherlands
Tel: 31 252 228 588
Email: holland@iconics.com

Czech Republic

Tel: 420 377 183 420
Email: czech@iconics.com

France

Tel: 33 4 50 19 11 80
Email: france@iconics.com

China

Tel: 86 10 8494 2570
Email: china@iconics.com

Italy

Tel: 39 010 46 0626
Email: italy@iconics.com

UK

Tel: 44 1384 246 700
Email: uk@iconics.com

India

Tel: 91 22 67291029
Email: india@iconics.com

Germany

Tel: 49 2241 16 508 0
Email: germany@iconics.com

Australia

Tel: 61 2 9605 1333
Email: australia@iconics.com

Middle East

Tel: 966 540 881 264
Email: middleeast@iconics.com

Microsoft Partner

Gold Application Development

Microsoft Partner

2014 Partner of the Year Winner
Public Sector: CityNext



www.iconics.com