



z/OS INTEGRITY SUITE

Information Systems security, integrity and availability are all predicated on controlling system changes. The NewEra Software z/OS Integrity Suite provides proven methods for finding potential problems and managing configuration content all while ensuring that your technical support staff has unfettered access to z/OS configuration components.

The NewEra Software z/OS Integrity Suite

The objective of the NewEra z/OS Integrity Suite is to ensure availability and prevent a denial of service. Its diagnostic and monitoring capabilities will detect z/OS component changes and alert users to all changes, especially changes that introduce problems. It provides tools to pinpoint and repair the problems, including the extremely rare cases where z/OS or its subsystems are completely unavailable.

To accomplish this, NewEra has developed the technology to execute, on demand or at scheduled intervals, a “Virtual IPL” of any z/OS Sysplex, System or Subsystem and, if needed, initialize a Stand Alone repair environment. These processes, performed by the NewEra z/OS Integrity Server, are divided into three major components: z/OS Configuration Inspection, z/OS Content Supervision and z/OS Configuration Repair and Recovery.

z/OS Configuration Inspection:

System availability can be adversely affected by the best-intended actions of your technical support staff. An alteration to a z/OS configuration component, perhaps a simple edit to a ParmLib, ProcLib or Subsystem Member, required to effect a system change, can introduce an instability that will only become apparent during the next “Real IPL.” Why? Two reasons: One, today’s best designed and implemented z/OS change management systems have **no way of closing the change loop** in a way that will determine that authorized changes were actually implemented. Two, without an on demand “Virtual IPL,” there is simply **no way to test** even the simplest configuration change to a running production system, no matter the management control process.

Using the NewEra z/OS Integrity Server, a detailed z/OS Configuration Inspection will take less than a minute to complete. The process begins as the NewEra Integrity Server **automatically discovers** the start of the z/OS IPL Path. Once on that path, the system release level, up to and including z/OS 1.7, is determined. The necessary **Integrity Rule Sets** that match the actual release level of the system under evaluation are selected and invoked. The Integrity Rules in the Rule Sets can be broadly divided into two distinct classes: **z/OS Path Rules** and **z/OS Component Rules**.

z/OS Path Rules direct the NewEra z/OS Integrity Server to faithfully invoke the same logical processes that z/OS would during a “Real IPL.” This results in the evaluation of the thousands of possible paths available but the selection of only one unique path, perhaps the only one applicable, to the z/OS Sysplex, System or Subsystem under evaluation. Because a z/OS configuration change **can force an IPL Path change**, the ability to **dynamically discover** the real logical path is vital to server process integrity.

z/OS Component Rules are called and applied as individual components are discovered in a sub process called **Component Inspection**. The Nucleus Initialization Members LOADxx, IEASYMxx and IEASYSxx are evaluated so that the actual prevailing OS Release Level, ParmLib Datasets, System Symbols and IEASYSxx members can be determined, filtered, resolved and consolidated. The final consolidated set of IEASYSxx Keywords leads to Prevailing ParmLib Member Inspections, which in turn leads to the inspection of command processes and the start and inspection of the major z/OS subsystems JES2/3, VTAM and TCP/IP. Of course, component inspections include more than just applying the unique syntax rules for each possible ParmLib Member or subsystem configuration; they focus as well on **Referential Integrity**. This latter process is designed to ensure, for example, that any referenced Volume, Dataset, Module or Member would be currently available to z/OS in a “Real IPL,” perhaps for APF and PPT Table creation. It will ensure, as well, that the aggregate requirements for system symbol memory and system dataset extents fall within acceptable ranges.

z/OS Content Supervision:

Actions that preserve and control the content of a z/OS Configuration are increasingly required as they can directly effect an overall improvement in z/OS operational integrity. This notwithstanding, the need for access to z/OS configuration components by your technical support staff will often fully or partly justify an escape from the more common methods used to ensure **Resource Access Control** over system components. z/OS Content Supervision offers two **Noninvasive Methods**, one passive and the other active, both of which result in a dramatic improvement in management oversight: z/OS Configuration Blueprints and Configuration Access Control.

A **Noninvasive Method** of system control is one that does not require the often-stated application



requirements for system authorization, system hooks or the front ending of configuration components.

Using the NewEra z/OS Integrity Server, Content Supervision begins as a **byproduct of component identification** along the IPL Path and ends with the creation of a z/OS **Configuration Package** containing a **Configuration Blueprint**. A new Blueprint, which contains a detailed description of the IPL Path and the content of each related configuration component, is created during each "Virtual IPL" and saved for future use. If directed, the NewEra z/OS Integrity Server will compare Blueprints to determine changes in the IPL Path and configuration components. Because the Blueprint contains only the **Prevailing** configuration components, attention can be immediately focused on changes to **what is important**; that is, what will actually be used in an IPL. While changes to non-prevailing components would be **considered noise** to some, other will take them equally seriously; we do as well. Optionally therefore, the **Blueprinting Process** can be extended to include all possible configuration components including Load Modules.

Controlling the access to z/OS configuration components is a serious business that should never result in a single point of entry. But just because multiple entry points are a requirement does not mean that a **Preferred Point of Entry*** cannot not be created and approved by management. Violations of that entry point can be noted and reported when other points of entry are used. Users of the NewEra z/OS Integrity Suite can optionally extend z/OS Content Supervision by naming the **Control Editor** as their preferred point of entry for altering configuration components. When implemented in conjunction with generally available Resource Access Systems, the **Control Editor** immediately turns System Datasets into **Controlled Datasets** and their content into **Controlled Members**. This noninvasive, though active approach captures change history - Who? What? When? Where? - and generates before and after copies of the edited controlled member.

If directed, the NewEra z/OS Integrity Server will compare controlled members to detect changes made using other edit methods. Discovered deviations from the preferred point of entry are considered **Audit Violations**.

Audit Violations refer to changes made outside the **Control Editor** environment. When they occur, management can refer to the hierarchy of preferred points of entry and direct users to make their changes inside the **Control Editor**.

*Preferred Entry Points - Integrity Hierarchy	Best Practices
1 - When system is running optimally	Control Editor
2 - When system may be compromised but TSO is running	ISPF
3 - When system may be compromised but TSO is down	NoTSO
4 - When system is down	SAE



z/OS INTEGRITY SERVER

Z/OS Configuration Repair and Recovery

In spite of Best Practices, at times systems fail. Stand Alone Environment (SAE) is a self-contained, self-loading system environment that provides immediate access to z/OS configuration components via an ISPF-like editor, **when MVS is down**. It IPL's from DASD, Tape or CD in a matter of seconds providing access to users through its own communications subsystem.

SAE has five integrated applications:

1. **Action Services** – A full screen ISPF like Editor that works with the NewEra Integrity server to assist in locating problems, identifying recent changes and making repairs;
2. **Image Services** – Provides access to NewEra Integrity Server and Inspection Reports and Blueprints.
3. **Stand Alone Restore** – Restores services at the volume, dataset or member level from volume backups created with either DFSSS or FDR;
4. **Hardware Confirmation** – When hardware is reconfigured this application validates sense data from the configurations without the need for an IPL;
5. **Fast DASD Erase** - An indispensable application for use at the end of Disaster Recovery (DR) tests or when decommissioning DASD. It not only clips the VTOC, it completely destroys all data by writing binary zeroes or a user-selectable pattern over your critical data. A set of integrated audit reports assist in compliance requirements and easily satisfies the most stringent internal and external audit demands.



Standards for z/OS System Management

Corporate Headquarters

Morgan Hill, California 95037
800 421-5035
TEL: 408-201-7000
FAX: 408-201-7099
email: info@newera.com

International

Fitz Software & Co.
TEL: +353.21.483.2131
email: mfitzgerald@fitzsoftware.com

UBS Hainer GmbH
TEL: +49-6641-65510
email: netinfo@ubs-hainer.com

Log-On Software, Ltd.
TEL: 972-3-576-3133
email: werner@log-on.com

Hi-End Consulting
TEL: 34-91-2938971
email: angel.gomez@highend-consulting.com

NewEra Software z/OS Integrity Suite Benefits

Benefits to Management	Benefits to Technical Staff
Provide tools to enable support staff to make changes in a controlled environment	Provides unfettered access to system datasets to make changes necessary for system enhancements and improved productivity
Reports on system integrity proactively, assures management that system will IPL	Reports on system integrity proactively, allows staff to research and fix problems indicated in reports
Generates reports alerting management and support staff of changes as well as the disposition of changes	Generates reports alerting management and support staff of changes as well as the disposition of changes
Allows for reports to be sent via email or TSO Broadcast that are of interest only to management	Allows for reports to be sent via email or TSO Broadcast that are of interest only to support staff
Works with conventional Security tool to ensure only authorized staff can make changes	Allows support staff to do their jobs with same security profile as always
Provides recovery tool in a controlled environment	Provides recovery tool to quickly recover from partial system outages
Provides control over changes made to ensure they are in accordance with policies and standards	Allows support staff to make changes in accordance with policies and standards
Generates Control Journal, which captures details of all significant change events	Control Journal points out changes and provides internal edit capabilities to correct problems
Automates data collection transparently	Allows support staff to continue accessing components as before
Combines with IFO Control Editor to provide complete picture of all members in PARMLIB	Helps support staff to prepare for IT audits
Assures management that quick recovery is possible	Provides tools and information necessary to recover quickly
Helps meet government requirements for the protection of personal information	Fast DASD Erase provides users with more time to test at DR Test; generates report proving all data erased.