



SYSchange

Protect system software integrity

w w w . m a i n s t a r . c o m

SYSchange protects your system software with a secure and accountable process for implementing member changes – and automates changes between sites.

- ▶ Manage changes easily and effectively
- ▶ Reliably recover from undesired or problematic changes
- ▶ Create an audit trail of changes at the member level
- ▶ Protect DASD volumes from unauthorized updates
- ▶ Establish repeatable processes for authorized users to make the right member-level changes

What happens when a change is made to your system libraries and critical path software for the operating system and other system software components? How do you manage these changes – and recover quickly if there is a problem?

SYSchange protects your critical software, backs up every changed member, and provides change control at the member level. Now you can automatically manage, document, back up, and audit member changes from a central point of control.

Safeguard system software – automatically

With consistent, automated processes, you can take control of your environment and minimize downtime. Plan changes and distribute them automatically to keep multiple sites in synchronization. Provide exactly the right level of authorization for users and implement an efficient approval process for better communication, higher integrity, and fewer system outages. Compare your disaster recovery and home site data sets and members to ensure that you have the software you need. If a change is problematic, recover to a “before” update member version quickly online. Need to meet internal or external audit requirements? SYSchange automatically provides audit trails and detailed reports.

Automatically Back Up and Recover Member Versions

Every change made to critical libraries can be tracked and automatically backed up when the change is made to ensure the member can be reliably recovered in the event of undesired changes.

SYSchange automatically backs up and records the involved members in the SYSchange VSAM Data and Control files.

Backups can be augmented by a user-supplied comment at the time the change is introduced to provide an audit trail and easy version identification in case recovery is required.

Protect Software Assets

SYSchange protects critical data sets and library members from unauthorized changes. Protection is available at the data set level for an entire DASD volume, or at the member level to protect critical members. The combination of data set level and member level protection provides data centers with complete protection around the clock.

The combination of data set level and member level protection provides data centers with complete protection around the clock.

Data Set Level Protection by Volume

SYSchange provides the capability to protect one or more DASD volumes (e.g., SYSRES) from unauthorized updates.

SYSchange allows only pre-designated “Super Users” to have ultimate authority to update the data sets on the protected volumes. Any data set level update attempts by anyone who is not a “Super User” will be automatically rejected.

Member-Level Protection

When a data set is protected by SYSchange, none of the members of that library can be changed by any user, unless SYSchange Checkout standards are used. This provides organizations the assurance that their critical libraries and members are protected from the security risks associated with unauthorized changes and unplanned downtime. To allow access to a certain member in a library, a member can be explicitly checked out by the SYSchange Global Administrator to a designated user. After the changes have been made to the member, the member is checked in by the user

along with a user-supplied comment. As an added safety feature, every time a checked-out member is updated, the SYSchange started task, monitoring all changes, automatically backs up the changed member, and records the change incident.

Request and Implement Planned Changes

Planned changes can now be safely and easily implemented to reduce the risks associated with undesired and unauthorized changes and accidental regression.

In the SYSchange Change Request (CR) Process, a user must first create a change request. A manager is then notified via the MVS TSO SEND command to review and approve the change request. After approval, the involved member(s) are automatically checked out to the pre-designated user/programmer defined by the CR. The changes are then made by the respective users/programmers. After completion, the Checkin feature is used to check in the involved member(s). When the last member has been checked in, SYSchange can be set up to automatically create a Promotion Package of the CR for distribution to other systems (local or remote).

Audit and Check Software Integrity

This feature of SYSchange provides mass comparisons of libraries to quickly identify library differences across the world, across town, or within your site. Once identified, an exception report is produced that identifies which data sets, PS, DA, or members of a PDS or PDSE are the same, different, or mismatched.

Lack of change (RC=0) indicates that the environment has remained intact, and hence the integrity is assured because no changes have been introduced. Various approaches can be used concurrently to achieve the desired goals.

With SYSchange, you can create repeatable process and controls to ensure that authorized changes are made only by authorized users, and that they can be easily audited.

Integrity Verification for a Large Local Environment

To perform Integrity Verification for a large environment such as your Production Site, use SYSchange to establish a “content reference” for the specified data sets (PS, DA, and PDS / PDSE members).

Optionally, critical libraries can be protected with the SYSchange Protect a Resource feature. Then, you can audit the changes recorded real-time by the SYSchange Started Task (STC) to identify who made the change, what action was involved (ADD, UPDATE, DELETE, RENAME, or ZAP), when the change was made, and which programs were responsible for the change.

Even if the libraries are not protected, you can audit the changes with SYSchange.

Integrity Verification Between Two Environments (Local or Remote)

A similar approach can be used for integrity verification between two environments (local or remote). One can imagine a scenario in which the user needs to verify whether their production software and their disaster recovery software are identical. For any two environments, SYSchange quickly identifies any data sets which have differences, such as mismatched members or members with different contents.

Use SYSchange to establish a “content reference” for the specified data sets (PS, DA, and PDS/PDSE members).

Then, transfer the set of SYSchange VSAM files (Data File and Control File) containing the “content references” from the production system to your disaster recovery system. Run SYSchange on your disaster recovery system to report missing members (source, load, JCL, panels, etc.), as well as any members with different contents. Using this methodology, you can ensure that your organization will be able to successfully resume business with the latest level of software when disaster strikes. This process requires the least amount of time and resources to get the job done. Due to the high performance of this operation and the minimal impact on the system, it can be performed as

With SYSchange, you can create repeatable process and controls to ensure that authorized changes are made only by authorized users, and that they can be easily audited.

often as necessary.

Distribute Software Changes

Automatically identify and package all or selective changes.

Automatic Identification and Packaging of Changed Members

Automatically identify and package any changed members (added, updated, or deleted) within a group of data sets previously identified to SYSchange without manual intervention.

SYSchange identifies, packages, and optionally distributes changed members and data sets across local or remote environments. The changed components (source, load, JCL, panels, etc.) are copied into a “Promotion Package” ready for transfer.

Customized Packaging of Changed Members

Selectively copy desired members from several desired libraries into a Promotion Package.

Freely decide which members of PDSs or PDSEs are to be copied into the custom Promotion Package. Select members from the desired libraries through an interactive process. After the Promotion Package has been received on the recipient system, the recipient of the Promotion Package can review the contents and decide what action to take

– promote all or only selected components.

Find Out More

Visit www.mainstar.com for technical articles and additional information on how SYSchange and Mainstar’s other innovative data access solutions can help you. To arrange a personal briefing or a free trial, contact us at product_info@mainstar.com.

Product Specifications

OS/390 and z/OS operating systems.

Mainstar is a registered trademark of Mainstar Software Corporation. SYSchange is a registered trademark of Pristine Software. All other products or company names are used for identification purposes only and may be trademarks of their respective owners. 003-0101-02 (01/24/07)

Copyright ©2007 Mainstar Software Corporation. All Rights Reserved. Mainstar Software Corporation is a wholly owned subsidiary of Rocket Software, Inc.

Why SYSchange?



Feature	What It Does	Benefit
Change tracking	Tracks all changes made to critical libraries, including information on who made the change, when the change was made, what changed, and why the change was made.	Coordinate changes easily and effectively and create an audit trail.
Change backups	Automatically backs up changes made to critical libraries.	Reliably recover from undesired or problematic changes.
Data set level protection by volume	Allows only pre-designated "Super Users" to have ultimate authority to update the data sets on the protected volumes.	Protect DASD volumes from unauthorized updates.
Member-level protection	Provides a safe, efficient way to approve changes and automatically check out the right members to the authorized users.	Simplify the process of authorizing the right users to make the right member-level changes.
Change Request Process	Creates a consistent, reliable process for implementing planned changes and not allowing unauthorized changes.	Reduce the risks associated with undesired and unauthorized changes and accidental regression.
Integrity verification	Compares libraries – such as your home site and disaster recovery site – to quickly identify differences and create reports.	Ensure you have the software you need at your disaster recovery site.
Change identification and packaging	Provides automatic or customized packaging of changes for updates to other systems, so you can synchronize multiple sites effortlessly.	Improve productivity while supporting business resiliency.
Online member-level recovery	Simplifies the process of recovering members based on documented changes.	Ensure that the correct version level of the member is recovered.