CADCAM INTEGRATION

The Most Informed Manufacturing Businesses Choose ShopFloorManager

30 years Providing Solutions for Manufacturing!
Phone: 1-781-933-9500 Download ShopFloorManager
Fax: 1-781-494-9585

Machine Monitoring <=Select
Machine Monitoring Search

SystemSecurity™ PDF-Version
A Complete Enterprise Security Base Module
Includes Configurable Security for Access to DNC Files, Documents, & ShopFloorManager™ Modules
Includes Configurable Events with Event Triggers for Capturing File & Document Changes
Part of an Integrated Family of ShopFloorManager™ EventAware™ Modules
Supports Windows 8™, Windows 7™ & Windows™ XP including Support for Terminal Server 2003/2005/2008

SystemSecurity™

SystemSecurity allows setting any Level of Security that your company requires by providing Customer Definable User Groups, User Group Rights(over 130 Rights in 11 different categories), Users, Logins & Passwords, Virtual File Cabinets, Resource Collections, restricted "Views" in User Configurable Combinations. These will provide any level of Security that a Company may require.

Set the desired Security Level by Creating the required number of User Groups in your Company, setting User Group Rights, adding any number of Users, Resources & ISO Sign-Off States to these User Groups. Users inherit their combined User Group Rights based on the User Groups they belong to which allows them to Access ShopFloorManager's Specific: Features, Data, Resources, Information, Files, Documents, etc.

In order to meet ISO9000 Document & File Change Security, SystemSecurity Captures any Document Change Events(Customer Configurable) that are generated when making Changes to Files & Documents. You can also activate the "Reason Required Feature" which will require User to enter a reason(s) for changing any Documents & files. When the Event is triggered a User is presented with a Customer Configurable List of Change Reasons and an input screen to enter a brief description of these Changes. You can then use ShopReports to generate a detailed Document & File Change Report!

SystemSecurity™ Protecting your Database, Files, Documents, Packets, Data & Information!

SystemSecurity™ **User Login/Logout** **And Passwords**	**System Provides your Company with Secure User Logins:**	

- Administrators Creates User Names
- Administrators Creates User Passwords
- Administrators Creates User Group Login/Logout Timeouts
- Administrators Selects User Group Categories and Configures Categories' Rights
- Administrators Creates any number of Users
- Administrators Creates User Groups with Rights that Control User's Access
- Administrators Can Configure over 130 Rights in 11 Different Categories

SystemSecurity's™ Basics

SystemSecurity's™ Basics Include:
- Login & Password Protection
- Creatable User Groups with 11 Different Rights Categories
- Creatable Users to Associate with User Groups
- Creatable Approval Sign-Off States to Associated with User Groups
- Creatable Resource Collections to Associated with User Groups
- **Note:** Resource Collections contain DNC Files & Packets and are associated with Machine Tools that have access to these DNC Files!
- Creatable Machine Tools which are associated with specific Resource Collections
- Over 130 Cross Integrated Individual Rights
- Customer Creatable Document/NC File/Packet Change Reasons
- Customer Activated Events for Document Change Events
- Virtual File Cabinets Access
- Reports for Verifying All Documents/NC Files/Packets Change Histories

User Group Rights Categories

SystemSecurity™ 11 User Group Rights Categories:
- All(130 Rights)
- Controlled Documents(25 Rights)
- DNC Files(52 Rights)
- File Cabinet(5 Rights)
- Machine(5 Rights)
- Management(8 Rights)
- Miscellaneous(9 Rights)
- DNC Editor(2 Rights)
- Packets and DNC Combined(3 Rights)
- Packets(25 Rights)
- User Interface Text Management(5 Rights)

Note: By selectively setting Rights in these various Security Categories you control the "Access" Level of Users in this User Group. Couple this with juridical use of Resource Collections & Sign-Off States you have complete and full control of Security for all of Documents, Files & Data.

Configurable Change Reasons

SystemSecurity™ Create Document/NC File/Packet Change Reasons
- Create New Reasons
- Retire Old Reasons
- Recover Old Reasons
- Sort Reasons By Id
- Manually Sort Reasons

Note: A Company can create any number of Specific "Document Change Reason Forms" from which a User can select when prompted by ShopFloorManager for Events that occur when making Changes, Deleting, Viewing, etc. to Documents/Files. These Forms also provide an area for entering an explanation for these "Changes" and is then stored in the History Change Database.

Change Events Activation

SystemSecurity™ Activate Specific Change/Reason Events
- Activate any of 77 Events for DNC Files
- Associate a Limited Set of your Change Reasons to a Specific Event for a DNC File
- Activate any of 23 Events for Controlled Documents
- Associate a Limited Set of your Change Reasons to a Specific Event for a Document
- Activate any of 21 Events for Packets
- Associate a Limited Set of your Change Reasons to a Specific Event for a Packet

Note: A Company may not want to have ShopFloorManager Prompt them every time an Event happens. SystemSecurity allows you to select Events to which a User is to Respond. Note however that even if a User isn't required to respond to an Event this Event is still recorded in ShopFloorManager's History Database.

Secure Virtual File Cabinet

SystemSecurity™ User Group Secure File Cabinets
- Create any number of File Cabinets
- Create any number of Draws, Folders, Sub-Folders within a File Cabinet
- Establish Security on any File Cabinet, Draw, Folder or Sub-Folder
- Drag, Drop & Move File Cabinets, Draws, Folders & Sub-Folders
- Turn-On/Off File Cabinets views as needed
- Securely Drag & Drop Documents/Files from with-in or external to ShopFloorManager

Note: Optionally using ShopFloorManager's Virtual File Cabinets provides another Level of Security by restricting "Access" to DNC Files, Documents & Packets that are contained in a File Cabinet Draw to which selected Users have access Rights. Virtual File Cabinets also provides a Sophisticated Management Tool for controlling all of a Company's Files/Documents/Packets.

Resource Collections

SystemSecurity™ User Group Specific Resource Collection(s)
- Associate with DNC Files
- Associate with Machine Tools
- Associate with Packets
- Resource Collection Security Properties
- Securely Drag & Drop NC File(s) from with-in or external to ShopFloorManage

Note: For Users who need access to DNC Files, Packets & Machine Tools, Resource Collections not only provide a way to segregate the Correct "DNC File to Machine Tool Relationships" but provide another Level of Security so only those Users who should have "Access" to these Files, Packets & Machine Tools do have "Access".

Sign-Off States

SystemSecurity™ User Group Specific Sign-Off States
- Sign-Off States Associate with Sign-Off User Groups thus Users
- Sign-Off Flow Charts that contain Sign-Off States
- Sign-Off Flow Charts that can be Associated with DNC Files
- Sign-Off Flow Charts that can be Associated with Controlled Documents
- Sign-Off Flow Charts that can be Associated with with Packets

Note: For Users who are restricted to accessing to DNC Files, Documents & Packets that have reached at a particular Approval Level the use of Sign-Off States provides another Level of Security.

Putting All Together

SystemSecurity™ How it Works
Security starts with the User Group(s) in which a particular User(s) belongs). The User(s) inherits the Specific Rights Configured from the 11 Categories for each of the User Groups within which they belong.

Using DNC Files as an example we note that even though a Particular User(s) may have Specific Rights to Manipulate DNC Files if this User is not part of a User Group that has access to the Resource Collections which contain the DNC Files they need, they will not be able to "Access" them.

If a User needs to Communicate with a Particular Machine Tool they will not only need access to the Resource Collection containing the required DNC Files but the Machine Tool will need to be Associated with this Resource Collection.

Further if Virtual File Cabinets are used then this User must also have Rights to a Particular File Cabinet associated with the Files to which they need Access.

Further if Approval and Sign-Off is used the only way a User can access an Unapproved NC/File is to be part of a User Group that is associated with a Sign-Off State where that File is in a Pending Approval State. See ISOApproval for more details!

You can have any Level of Security from "None" to "All" as dictated by your Company's Policies.

Note: Documents' and Packets' Security is handled similarly.