

Information Bulletin

No: 12-4-02

Category: Operator Control Station

To: Distribution

OCS System Security

Summary

There are multiple levels of security included in the Cscape™ programming software and the Operator Control Station (OCS) equipment. **System Security** offers four levels of password protection. **OEM Code** offers protection for selected sections of ladder logic. And, there is a **Password Data** field available to prevent access to selected display screens and data fields.

System Security

In any industrial control system such as those created by Cscape, some manner of security must be maintained. Shop Floor personnel generally should not be able to load, view, or change programs. Programming personnel may need limited access to the system, but are not usually allowed access to the security system. A single System Administrator should have access to all functions.

User Definable Permissions

Cscape provides an “open” security system. Four levels are provided: “Administrator” and three others. Administrator automatically has access to all permissions, including changing the passwords. The name and available permissions for each of the “secondary” levels are user programmable. You are not “stuck” with the functions and levels that someone else thinks are useful; you can define the access for each of the three security levels to best suit your installation and needs.

Hardware Protection

Cscape also provides a level of hardware security for controllers. This includes the ability to Start or Stop the controller; and the ability to set the controller's Network ID on those controllers that accept this feature (like the OCS100 and OCS200).

Passwords

Like most security systems, different “levels” of security are accessed using a “password.” [In Cscape, all passwords are numeric.] The name assigned to the security level, the functions available to the security level, and of course the password for that level is user-definable.

An Administrator level is predefined. Users at this security level have access to all permissions, and may add or change passwords and their associated permissions. Users with the Administrator controller security level can change the password for this level.

The “secondary” levels are completely user-definable by a user with Administrator security level. One level might be assigned to a “Programmer,” who can read and write files, manipulate controller modes, etc. Yet another might be for the everyday “User,” who can monitor the program or change certain key values, but can't change either the source code file or the program within the controller through a download. He might not be able to change the controller mode (Run/Idle).

Administrator Level

The actions of the permission settings at the Administrator Level are slightly different than those of the Secondary Levels. At the Administrator Level, permissions are used to REQUIRE or IGNORE password protection. For example, if the Administrator checks the OPEN permission, then all Secondary Levels must provide a password in order to open the file. However, if the OPEN permission is not checked, then all Secondary Levels may open the file without security password clearance.

Secondary Levels

Permission settings at the Secondary Levels operate slightly different from those at the Administrator Level. If a Secondary Level permission is checked, then this function is allowed if the proper password is supplied. If the permission is not checked, then a user with this password is not allowed access to this function.

OEM Code

OEM Code is a feature unique to the OCS Product Line. With this feature, sections of code may be marked as “Original Equipment Manufacturer” (OEM) or “proprietary.” These sections are then password protected from viewing or editing. By being password protected from view, code secrets can be hidden from unauthorized personnel. Only a user with the proper security permissions and password can access code thus marked.

NOTE: The use of OEM Code requires that this feature be password protected using the above System Security feature. If OEM Code is NOT password protected, then the OEM Code settings are not available.

Password Data

Access to selected display screens, such as maintenance or setup screens, can be controlled through the use of the Password Data field. It allows a 32 bit unsigned integer password to be entered to the OCS register without displaying actual numeric characters. When editing, an ‘*’ will appear in the current digit position being inserted.

When editing is complete, all digit positions will be filled with an ‘*’ sign unless the current register value is greater than the number of digits. In that case, all digit positions will be filled with a ‘+’ sign.

Cscape is a registered trademark of Horner APG, LLC.

Horner APG, LLC

640 N. Sherman Dr. ~ Indianapolis, IN 46201 ~ Ph: 317-916-4274 ~ Fax: 317-916-4280

For additional information, please visit: www.HornerOCS.com