

10 Steps to Understanding the IGSS Access Control System

Many are not aware of the possibilities of the IGSS access control system and many find it difficult to understand. The following text will state a number of facts and show how to configure the system by a number of examples going through all the features in the system.

Each example will show a solution using a number of tables. Three tables will show the content of the three dialogues in the user administration program. Where it is relevant a fourth table will show how objects in the configuration are protected by protect objects. When “exclusive control” is shown yet another table will show the bindings between station names and protect strings. This is equivalent to the fourth dialogue in the user administration program.

Each example has as few features as possible to make them more readable. So when you start implementing your own access control solution you will most often need to combine several examples. For many of the examples the shown solution is one amongst many, so there is room for experimenting.

Simple Access control

- A user in the system is identified with a user name and a password
- A standalone user has no access rights in the system
- A user gets access rights by joining a group
- A user can join several groups if needed
- A group has the task to collect access rights and forward them to the members of the group
- The basic rights giving access to operate the system are set directly in the group.
- The basic rights are:
 - Administration: Access to user administration
 - Definition: Access to modify the configuration
 - System: Access to operate the run time system e.g. start/stop the configuration, data collection control etc.
- Access rights to operate the configuration are attached to the group by attaching protect objects to the group.

Example 1

Simple access control can be illustrated by the following example.
There should be three users on the system:

Admin: Can do anything.
Operator1, Operator2: Can do system operations and operate the configuration

Users:

User Name	Password	Member of group
Admin	Xxxxx	Administrators
Operator1	Yyyyy	Operators
Operator2	Zzzzz	Operators

Groups

Group Name	Can define	Can administer	Can use system commands	Has protect objects
Administrators	X	X	X	
Operators			X	

Protect objects

Protect object	Level	Ack	Set point	Alm. limit	Commands	String	Table	Area / diagram	Hierarchy

Objects protected by protect objects

Object protected	Protected by

Example 2

The same as example 1 but now we want to obtain rights from multiple groups.

Users:

User Name	Password	Member of groups
Admin	Xxxxx	DefAdmin System
Operator1	Yyyyy	System
Operator2	Zzzzz	System

Groups

Group Name	Can define	Can administer	Can use system commands	Has protect objects
DefAdmin	X	X		
System			X	

Protect objects

Protect object	Level	Ack	Set point	Alm. limit	Commands	String	Table	Area / diagram	Hierarchy

Objects protected by protect objects

Object protected	Protected by

Protecting Objects in the Configuration

- Any object in the configuration that should be protected must be protected by a protect object
- Any configuration is born with one protect object "Protect". More can be added if needed
- A protect object is actually a digital object that can have the following states:
 - 0: Unprotected
 - 1: Protect level 1
 - 2: Protect level 2
 - 3: Protect level 3
 - 4: Protect level 4
 - 5: Full protect
- Whenever you make an operation (Change process values, acknowledge alarm, open diagrams etc.) on a protected object the following will happen.
 - The state of the protect object is checked.
 - If it is "Unprotected" the operation is performed

- If it is "Full protect" the operation is rejected
- If it is "protect level 1, 2, 3 or 4" the user rights will be checked.
- For the levels 1, 2, 3 and 4 on each protect object you can specify a number of rights
 - Acknowledge alarms
 - Change set points
 - Change alarm limits
 - Issue commands
 - Change string values
 - Change values in tables
 - Open area and diagrams
- To make these rights available to a user the user must be member of a group that has the appropriate protect object and protect level attached.
- A group can be attached to several protect objects and levels

Example 3

This example will illustrate how access to an area can be protected by protect objects. Protecting an area or diagram will make it invisible to users not having appropriate access rights

In a configuration there are two areas, "Global" and "Restricted"

Define two users:

OP1 : Can operate both areas, and work as administrator

SV1: Can operate "Global" only.

Users:

User Name	Password	Member of groups
OP1	Xxxxx	Operator
SV1	Yyyy	Service

Groups

Group Name	Can define	Can administer	Can use system commands	Has protect objects
Operator	X	X	X	Protect level 1
Service				

Since the group "Service" do not have any rights it may as well be omitted. User "SV1" should not be member of any groups then. Including it will however make it more easy to make changes later on.

Protect objects

Protect object	Level	Ack	Set point	Alm. limit	Commands	String	Table	Area / diagram	Hierarchy
Protect	1							X	
Protect	2								
Protect	3								
Protect	4								

Objects protected by protect objects

Object protected	Protected by
Area "Restricted"	Protect

The protect object "Protect" should in this case be permanently set to level 1.

If you instead want to restrict access to individual diagrams you can still use this example you should just protect each of the diagrams with the protect object instead. This means that only the content of last table "Objects protected by protect objects" is changed.

Example 4

As an alternative to deny any access to a diagram/area you could give free access to view area/diagrams but restrict operations on vital objects.

In a configuration there are two vital objects Level_1 monitoring the level in a tank and pump_1 controlling a pump filling the tank.

The set point , alarm limits and acknowledging alarms of "level_1" and command issuing on "pump_1" should only be operated by a user working on the related process or a super user.

All other users in the system can not operate the two objects

Create three users:

Super: Has super user and administrators rights

OP1: Is the normal process operator

OP2: Is a guest operator

Users:

User Name	Password	Member of groups
Super	Xxxxx	Admin
OP1	Yyyyy	Operator
OP2	Zzzzz	Guest

Groups

Group Name	Can define	Can administer	Can use system commands	Has protect objects
Admin	X	X	X	Protect level 1
Operator				Protect level 1
Guest				

Since the group "Guest" do not have any rights it may as well be omitted. User "OP2" should not be member of any groups then. Including it will however make it more easy to make changes later on.

Protect objects

Protect object	Level	Ack	Set point	Alm. limit	Commands	String	Table	Area / diagram	Hierarchy
Protect	1	X	X	X	X				
Protect	2								
Protect	3								
Protect	4								

Objects protected by protect objects

Object protected	Protected by
"Level_1" in area "Global"	Protect
"pump_1" in area "Global"	Protect

The protect object "Protect" should in this case be permanently set to level 1.

Hierarchy

In the above example a user either had any right on an object or none. Quite often you want to differentiate so you have a number of users with different rights to operate the objects. In this case you can use the hierarchy feature on the protect objects.

Hierarchy make the protect object appear as if it is more than one state at the same time.
The following setup:

Protect objects

Protect object	Level	Ack	Set point	Alm. limit	Commands	String	Table	Area / diagram	Hierarchy
Protect	1								
Protect	2								
Protect	3								
Protect	4								X

Will give the following effects:

If “Protect” is in level 4 the check mark in “Hierarchy” will make both level 4 and level 3 active levels

If “Protect” is in level 3 only level 3 will be active. Same in level 2 and 1.

The following setup:

Protect objects

Protect object	Level	Ack	Set point	Alm. limit	Commands	String	Table	Area / diagram	Hierarchy
Protect	1								
Protect	2								
Protect	3								X
Protect	4								X

Will give the following effects:

If “Protect” is in level 4 the check marks in “Hierarchy” will make both level 4, 3 and 2 active levels

If “Protect” is in level 3 only level 3 and 2 will be active.

If “Protect” is in level 2 only level 2 will be active.

Example 5

We use the same setup as in example 4 but change the requirement a little

The set point and alarm limits of “level_1” should now only be operated by a super user.

Operating “pump_1” and alarm acknowledging on “Level_1” should only be operated by a user working on the related process or a super user.

All other users in the system can not operate the two objects

Create three users:

Super: Has super user and administrators rights

OP1: Is the normal process operator

OP2: Is a guest operator

Users:

User Name	Password	Member of groups
Super	Xxxxx	Admin
OP1	Yyyyy	Operator
OP2	Zzzzz	Guest

Groups

Group Name	Can define	Can administer	Can use system commands	Has protect objects
Admin	X	X	X	Protect level 4 Protect level 3
Operator				Protect level 3
Guest				

Since the group "Guest" do not have any rights it may as well be omitted. User "OP2" should not be member of any groups then. Including it will however make it more easy to make changes later on.

Protect objects

Protect object	Level	Ack	Set point	Alm. limit	Commands	String	Table	Area / diagram	Hierarchy
Protect	1								
Protect	2								
Protect	3	X			X				
Protect	4		X	X					X

Objects protected by protect objects

Object protected	Protected by
"Level_1" in area "Global"	Protect
"pump_1" in area "Global"	Protect

The protect object "Protect" should in this case be permanently set to level 4.

Process Controlled Access Control and Multiple Protect Objects

Until now the protect object has always been in a fixed state, but since the protect object basically is a digital object its state and there by the access rights of the users may as well be controlled by the process.

Example 6

A plant is working in two shifts. In the day shift there are full production and in the evening parts of the production are closed down. Each part of the production has its own area in the configuration – Prod_1 and Prod_2.

The operators should only be able to access areas relevant for the current shift, so Prod_2 should not be accessible for the evening shift

There is one operator for each shift OP_day and OP_evening

Administrators should however be able to access everything unconditional.

The shifts are controlled from the PLC.

Users:

User Name	Password	Member of groups
Super	Xxxxx	Admin
OP_day	Dddd	Day

OP_evening	Eeeee	Evening
------------	-------	---------

Groups

Group Name	Can define	Can administer	Can use system commands	Has protect objects
Admin	X	X	X	Protect level 1
Day				Protect level 2
Evening				

Protect objects

Protect object	Level	Ack	Set point	Alm. limit	Commands	String	Table	Area / diagram	Hierarchy
Protect	1							X	
Protect	2							X	X
Protect	3								
Protect	4								

Objects protected by protect objects

Object protected	Protected by
Area "Prod2"	Protect

The protect object will be in level 2 in the day shift and level 1 the rest of the time

Example 7

Illustrating multiple protect objects

The scene is the same as in example 6 now we just want to make a minor change.

The day shift operators should only be allowed to see the area Prod_2 and the evening shift operator only the area Prod_1.

For this solution we introduce a protect object for each part of the production

Users:

User Name	Password	Member of groups
Super	Xxxxx	Admin
OP_day	Ddddd	Day
OP_evening	Eeeee	Evening

Groups

Group Name	Can define	Can administer	Can use system commands	Has protect objects
Admin	X	X	X	Protect_1 level 1 Protect_2 level 1
Day				Protect_2 level 2
Evening				Protect_1 level 2

Protect objects

Protect object	Level	Ack	Set point	Alm. limit	Commands	String	Table	Area / diagram	Hierarchy
Protect_1	1							X	

Protect_1	2							X	X
Protect_1	3								
Protect_1	4								
Protect_2	1							X	
Protect_2	2							X	X
Protect_2	3								
Protect_2	4								

Objects protected by protect objects

Object protected	Protected by
Area "Prod1"	Protect_1
Area "Prod2"	Protect_2

The Protect_1 will be in level 1 at the day shift and level 2 at evening shift
The Protect_2 will be in level 2 at the day shift and level 1 at evening shift

Exclusive Control

As a supplement or alternative to protecting the configuration on a user level you can protect on station level. This is called exclusive control. It is mostly used in multi-user systems where you want some operator stations to have limited functionality.

- To protect objects using exclusive control the object must still be protected by a protect object.
- The protect object must be connected to a string object
- When an operation is performed on the protected objects the content of the connected string object will be compared to the content of a string table
 - For each string in the string table a network name of an operator station can be listed.
 - If the string is not found in the table or the name of the operator station does not match nobody can do the operation on this operator station
 - If the string is found and the name of the operator station match, the operation can be performed on the actual operator station.
- After the operator station has been authorized for the operation, user level rights are checked.

Example 8

You have a multi-user system. In the configuration everybody should be able to see the area "Common" while the area "Restricted" must only be seen on two operator stations placed in restricted areas. These two operator stations have network names "RESOP1" and "RESOP2".

Users:

User Name	Password	Member of groups

Groups

Group Name	Can define	Can administer	Can use system commands	Has protect objects

Protect objects

Protect object	Level	Ack	Set point	Alm. limit	Commands	String	Table	Area / diagram	Hierarchy
Protect	1								
Protect	2								
Protect	3								
Protect	4								

Exclusive Control string table

String value	Network name
"Restrict"	RESOP1
"Restrict"	RESOP2

Objects protected by protect objects

Object protected	Protected by
Area "Restricted"	Protect

Protect objects connected to string objects

Protect object	Connected to string
Protect	ExclString

The string "ExclString" is set to have the fixed value "Restrict"

Example 9

Like the states of the protect object also the content of the connected string can be controlled from the PLC. In this case we can change the operations different operator stations can do over time.

It is also possible to have multiple strings match the same operator station.

The scene is the same as in example 8, but now we the plant is running in two shifts. In the day shift both RESOP1 and RESOP2 should see the area "Restricted" and in the evening, only RESOP2 should see it. The shifts are controlled by the PLC.

Users:

User Name	Password	Member of groups

Groups

Group Name	Can define	Can administer	Can use system commands	Has protect objects

Protect objects

Protect object	Level	Ack	Set point	Alm. limit	Commands	String	Table	Area / diagram	Hierarchy
Protect	1								
Protect	2								
Protect	3								

Protect	4								
---------	---	--	--	--	--	--	--	--	--

Exclusive Control string table

String value	Network name
"Restrict_day"	RESOP1
"Restrict_day"	RESOP2
"Restrict_evening"	RESOP2

Objects protected by protect objects

Object protected	Protected by
Area "Restricted"	Protect

Protect objects connected to string objects

Protect object	Connected to string
Protect	ExclString

The string "ExclString" is connected to the PLC. The PLC will send set the string to "Restrict_day" in the day shift and "Restrict_evening" in the evening.

If it sets it to something else in the night no operator stations will be allowed access to the area.

Example 10

We reuse the scene from example 8. Now the access to area "Restricted" should be even more limited. You have to be on one of the operator stations "RESOP1" and "RESOP2" and you have to be a super user

Users:

User Name	Password	Member of groups
SuperUser	Ssssss	Admin

Groups

Group Name	Can define	Can administer	Can use system commands	Has protect objects
Admin	X	X	X	Protect level 1

Protect objects

Protect object	Level	Ack	Set point	Alm. limit	Commands	String	Table	Area / diagram	Hierarchy
Protect	1							X	
Protect	2								
Protect	3								
Protect	4								

Object "Protect" is set permanently to level 1.

Exclusive Control

String value	Network name
"Restrict"	RESOP1
"Restrict"	RESOP2

Objects protected by protect objects

Object protected	Protected by
Area "Restricted	Protect

Protect objects connected to string objects

Protect object	Connected to string
Protect	ExclString

The string "ExclString" is set to have the fixed value "Restrict"