



Integriti

Programming Reference

Manual

Please send any comments on this manual to:
publications@innerrange.com

**INNER RANGE recommends that all Inner Range
systems be installed & maintained by
FACTORY CERTIFIED TECHNICIANS.**

**For a list of Accredited Dealers in your area
refer to the Inner Range Website.**

<http://www.innerrange.com>

Integriti Programming Reference.

Table of Contents

Generic Programming Operations	7
Permission programming (Qualify Pairs).....	7
Action programming.....	10
Action Type and Qualification settings.....	11
Action Entity settings.....	13
AREA or AREA LIST	13
AUXILIARY or AUXILIARY LIST	13
DOOR or DOOR LIST.....	14
FLOOR (LIST) and LIFT CAR (LIST).....	14
TRIGGER INPUT.....	15
SET AREA USER IS IN (User Location).....	16
SET AREA USER COUNT (Number of Users in Area)	16
SET INPUT COUNTERS.....	16
SIREN CONTROL.....	17
SET TIMER VARIABLE	18
SET GENERAL VARIABLE.....	18
CONTROL AIR-CONDITIONING.....	19
MACRO CONTROL.....	19
ISOLATE / SOAK TEST AN INPUT	20
COMMS TASK CONTROL.....	20
GRANT AMNESTY.....	21
SET AIR-CONDITIONER TEMPERATURE	21
Users and Permissions	22
User Codes.....	22
Permission Groups.....	24
Lists	26
Groups	27
MENU GROUPS.....	27

PROCESS GROUPS.....	30
Integriti Default Process Group Contact ID Event Codes and typical applications.....	35
INTERLOCK GROUPS	36
RF Remotes.....	36
RF Remote Templates.....	36
RF Remote operations supported	37
Card Templates.....	37
Apartments.....	38
Times.....	39
Time and Date.....	39
Time Periods	39
Schedules.....	40
Holidays	41
LCD Messages	41
Installer	43
Input Programming.....	45
Area Programming.....	48
Modules.....	53
LCD Terminal.....	53
Expander	57
2-Door Reader Module	58
Integriti Graphic Terminal.....	62
RF Expander	67
LAN Power Supply Module	68
Integriti Four Door Access Module (Not yet available)	70
Concept Analogue Module (Not yet supported)	71
Controller – Module Details	71
Controller – Connection Details	74
Concept Intelligent 4-Door Access Module	76
Communications Programming.....	86
Comms Tasks	86
INTEGRITI FORMAT	87
DIGITAL DIALLER FORMATS	91
GSM Comms Task Notes.....	95

GSM FORMAT	95
SMS Control	100
SMS Control Command Syntax.....	101
AUTOMATION FORMAT.....	103
EMS FORMAT.....	107
Introduction to Securitel Comms Task.	109
SECURITEL FORMAT.....	110
Introduction to the Intercom Comms Task.	112
INTERCOM FORMAT	112
Intercom Comms Task Kenwei Interface.....	113
SKY TUNNEL FORMAT	114
Telephone Numbers	115
Network Interface Controllers.....	115
DNS Servers	115
System Options Programming.....	116
Memory Configuration	116
Auxiliary Options.....	116
EOL Configurations	116
Access Control	118
Entity Types and Groups.....	118
DOOR TYPES.....	118
QUALIFIED DOOR TYPES	121
LIFT TYPES	122
QUALIFIED LIFT TYPES.....	124
Lift Group Programming	125
Access Control Entities	126
Card Formats	126
Door Programming	129
Roller Doors	133
Lift Car Programming.....	135
Floor Programming.....	136
Automation and Logic Functions	138
Named Actions	138
Macros	139

Air-conditioning	141
Comparisons	141
Compound Entities	143
General Variables.....	144
General Timers	144
Calibrations	145

Generic Programming Operations

Permission programming (Qualify Pairs)

Permissions allow relevant entities to be paired together to provide a simple and logical, yet flexible and powerful means of defining permissions or qualifying operations.

A Permission consists of a “What” entity (Qualifyee) and an optional “When” entity (Qualifier).

- “What” is an item or a list of items that will be allowed or denied, or that will be processed together in some way. e.g. “What” is typically an entity such as an Area, Area List, Door, Door List, Floor List, Menu Group, Input, User Action, etc.
- “When” is an optional item or list of items that will determine when the permission applies. i.e. Defines when the “What” entity will be used in the processing. e.g. “When” is typically an entity such as a Time Period, Schedule, Area, Input, Comparison, etc. The absence of a “When” entity implies that the permission “Always” applies.

When programming via the Integriti System Designer, Permissions or Qualify Pairs are given different titles depending on where they are applied.

e.g. When applied to User programming, they are called “Extra Permissions” or “Permissions”.

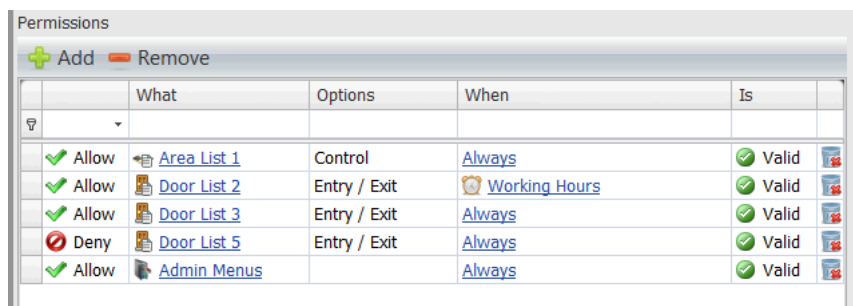
See the list below for how Permissions are described when they are applied to other entities.

In short, a Permission or Qualify Pair determines “what” entity is used in that permission or operation, and “when” it is used.

<u>This Number of Permissions:</u>	<u>Can be assigned to:</u>	<u>Where they are referred to as:</u>
8	Users	Extra Permissions
16	Permission Groups	Permissions
6	LCD Terminals	Extra Restrictions
2	Integriti Graphic Terminals	Extra Restrictions
16	Interlock Groups	Interlocked Entities
8	Qualified Door Types	Door Types
??	Qualified Lift Types	Lift Types
??	Lift Cars	Restricted Floors

Regardless of which of the above entities the Permissions are assigned to, a dialog box like the one pictured below is displayed.

- The “Allow or Deny”, “What”, “When” and “Is Valid/Invalid” columns are always available, regardless of the entity being programmed.
- The “Options” column is only available in User, Permission Group, LCD Terminal and Graphic Terminal programming, but might not be active, depending on the type of entity selected for the “What” parameter.



Option	Initial Screen / Option	Description
Allow / Deny		Select whether the entity that is to be defined in this Permission, is to be “Allowed” or “Denied” by this Permission. e.g. If a Door List is to be defined and this option is set to “Allow”, then those Doors will be allowed.
What	Door Door List Area Area List Floor Floor List. Lift Car Lift Car List Menu Group Permission Group User Door Type Lift Type Auxiliary Aux List Input	Select the entity to be used as the “What” for this Permission. The options listed opposite are the entities most likely to be used in this setting.
Options		Depending on the type of “What” chosen, options for that entity may then be available. Options are provided for Door, Door List, Area or Area List.
	DOOR / DOOR LIST OPTIONS Permit Entry Permit Exit	Entry / Exit Options Access via an Entry Reader is permitted. Access via an Exit Reader is permitted.
	AREA / AREA LIST OPTIONS On Off Grant Access to Area.	Area Control Options. On control (Arm) allowed. Off control (Disarm) allowed. Allow a User to gain entry through a Door into an Area that is allowed, regardless of whether the Door is allowed.
When		If the “What” entity selected is not “Always” allowed, you will need to select a “When” entity. e.g. Time Period, Area, etc. Refer to the table in the next option for a list of the entities most likely to be used in this setting.

Is	If a “When” entity is selected you now need to define how it will qualify the What entity. This is done by choosing the required option from the “Is” column. e.g. If a Time Period is selected and this option is set to “Valid”, then the “What” Entity will only be allowed when the Time Period is Valid. The following table shows the options available for the types of entities that might be used in this option. <table border="1"> <thead> <tr> <th>Valid / Invalid</th><th>Time Period / Schedule / Holiday</th></tr> </thead> <tbody> <tr> <td>Locked / Unlocked</td><td>Door</td></tr> <tr> <td>All Locked / Any Unlocked</td><td>Door List</td></tr> <tr> <td>Armed / Disarmed</td><td>Area</td></tr> <tr> <td>All Armed / Any Disarmed</td><td>Area List</td></tr> <tr> <td>Valid / Invalid</td><td>Floor</td></tr> <tr> <td>Valid / Invalid</td><td>Floor List</td></tr> <tr> <td>Valid / Invalid</td><td>Lift Car</td></tr> <tr> <td>Valid / Invalid</td><td>Lift Car List</td></tr> <tr> <td>Valid / Invalid</td><td>Auxiliary. (Valid = ON. Invalid=OFF)</td></tr> <tr> <td>Valid / Invalid</td><td>Auxiliary List</td></tr> <tr> <td>Valid / Invalid</td><td>Zone. (Valid = Sealed. Invalid=Unsealed)</td></tr> <tr> <td>Valid / Invalid</td><td>User</td></tr> <tr> <td>Valid / Invalid</td><td>LCD Message</td></tr> <tr> <td>Valid / Invalid</td><td>Named Action</td></tr> <tr> <td>Valid / Invalid</td><td>Macro</td></tr> <tr> <td>Valid / Invalid</td><td>Comparison</td></tr> <tr> <td>Non-Zero / Zero</td><td>General Variable</td></tr> <tr> <td>Running / Not Running</td><td>General Timer</td></tr> <tr> <td>Valid / Invalid</td><td>Compound Entity</td></tr> </tbody> </table>	Valid / Invalid	Time Period / Schedule / Holiday	Locked / Unlocked	Door	All Locked / Any Unlocked	Door List	Armed / Disarmed	Area	All Armed / Any Disarmed	Area List	Valid / Invalid	Floor	Valid / Invalid	Floor List	Valid / Invalid	Lift Car	Valid / Invalid	Lift Car List	Valid / Invalid	Auxiliary. (Valid = ON. Invalid=OFF)	Valid / Invalid	Auxiliary List	Valid / Invalid	Zone. (Valid = Sealed. Invalid=Unsealed)	Valid / Invalid	User	Valid / Invalid	LCD Message	Valid / Invalid	Named Action	Valid / Invalid	Macro	Valid / Invalid	Comparison	Non-Zero / Zero	General Variable	Running / Not Running	General Timer	Valid / Invalid	Compound Entity
Valid / Invalid	Time Period / Schedule / Holiday																																								
Locked / Unlocked	Door																																								
All Locked / Any Unlocked	Door List																																								
Armed / Disarmed	Area																																								
All Armed / Any Disarmed	Area List																																								
Valid / Invalid	Floor																																								
Valid / Invalid	Floor List																																								
Valid / Invalid	Lift Car																																								
Valid / Invalid	Lift Car List																																								
Valid / Invalid	Auxiliary. (Valid = ON. Invalid=OFF)																																								
Valid / Invalid	Auxiliary List																																								
Valid / Invalid	Zone. (Valid = Sealed. Invalid=Unsealed)																																								
Valid / Invalid	User																																								
Valid / Invalid	LCD Message																																								
Valid / Invalid	Named Action																																								
Valid / Invalid	Macro																																								
Valid / Invalid	Comparison																																								
Non-Zero / Zero	General Variable																																								
Running / Not Running	General Timer																																								
Valid / Invalid	Compound Entity																																								

Action programming.

Actions allow an entity to be programmed to provide direct control of another entity.

This eliminates the need to program separate intermediate logic operations to link these entities.

Actions can be programmed for entities such as:

- Zones and System Inputs (Alarm Action)
- Areas
- RF Remote Templates (Button Actions)
- RF Expanders (Feedback Action)
- Communications Tasks (Status Actions and Command-back Action)
- Named Actions
- Macros
- Comparisons

If an Action is not required to operate at all times, a Qualifier may be assigned to determine the conditions under which the Action will be enabled and disabled. e.g. A Time Period, an Area State, etc may be used to qualify the Action.

Regardless of which of the above entities an Action is programmed for, when the required Action option is expanded, a dialog box like the one pictured below is displayed.

This example is the “Entry Action” in Area programming.

User Counting	
Actions	
Close Action	
Entry Action	Control Aux List
Auxiliary List	Warning Bleepers × ...
Control Type	Normal
On Time	0 hours 00 mins 00 secs
Off Time	0 hours 00 mins 00 secs
Delay On	☐
Delay Off	☐
Update Dynamic Only	☐
When Asserted...	Turn On
When Disasserted...	Turn Off
Qualifier	×
Invert Qualifier	☐
Exit Action	
Zone Test Action	
Warning action	
Isolate Action	
Unseal Action	
General	

Programming is described in the following tables.

- The first table describes the programming options common to all actions.
- The second table describes the programming specific to particular entity types.

Action Type and Qualification settings

Option	Initial Screen / Option	Description
Action Type	None Control Area Control Area List Control Aux Control Aux List Control Door Control Door List Secure/Unsecure a floor on a lift car Secure/Unsecure a floor on a lift car list Secure/Unsecure a floor list on a lift car Secure/Unsec a floor list on a lift car list Trigger Input Set Area User is in Set Area User Count Set Input Counters Control Siren Set Timer Variable Set Variable Control Air-conditioning Macro Control Isolate Comms Task Control Grant Amnesty Set Air-conditioner Temperature	Select the Entity type that will be controlled or adjusted by the entity that you are currently programming. e.g. In Zone Input programming, this is the entity that will be controlled by the Alarm/Seal state of this Input. Control an Area (On/Off/Defer) Control an Area List (On/Off/Defer) Control an Auxiliary Control an Auxiliary List Unlock/Lock a Door Unlock/Lock a Door List Secure/Unsecure a floor on a lift car Secure/Unsecure a floor on a lift car list Secure/Unsecure a floor list on a lift car Secure/Unsecure a floor list on a lift car list Trigger an Input State Adjust the location of a nominated User. Adjust the number of Users currently in an Area. Adjust the current value of an Input event count. Control a Siren Trigger a General timer Trigger a General Variable Control Air conditioning zones Start/Stop a Macro Isolate a nominated Input Comms Task operation. E.g. Restart or Update. Reset all User Anti-Passback Area records. Adjust Temperature setting for a nominated Zone in a nominated Air-conditioning Unit.
Select the Entity to control.	The terminology specific to each entity type for this option is shown in the next table.	When the Action Type has been selected, the title of the next field will change accordingly and you can select the entity of that type. e.g. If “Control Aux List” is selected, the title of the next field will change to “Auxiliary List” and you can select from the Auxiliary Lists available in the system.

When Asserted / When De-asserted	The terminology for the options in this setting adjusts for the selected entity. The options specific to each entity type are shown in the next table.	The “When Asserted” option specifies the operation that will be performed on the selected entity when the action is asserted. e.g. 1. In Zone Input programming, this is the action that will occur when the Input goes into the “Alarm” state. 2. In the Area Close Action it is the action that will occur when the Area is turned On. The “When De-asserted” option specifies the operation that will be performed on the selected entity type when the action is De-asserted. e.g. 1. In Zone Input programming, this is the action that will occur when the Input goes into the “Seal” state. 2. In the Area Entry Action it is the action that will occur when the Entry Timer expires, or the Area is turned Off.
Qualify settings		Actions may be qualified by the state of another entity. e.g. An action may be programmed to cause a Door to be unlocked when an Area is Disarmed. A Time Period can then be used in the Qualify options for this action to ensure that the action will only occur during normal working hours.
Qualifier		Select the Entity to be used to Qualify the Action. e.g. Time Period, Schedule, Area, Auxiliary, etc. The Action will be allowed if the Qualifier is Valid. e.g. Time Period or Schedule is Valid Area is Off Door is Unlocked etc.
Invert Qualifier		Enable this option if the Action is required to be allowed when the Qualifier is NOT Valid. e.g. Time Period or Schedule is Invalid Area is On Door is Locked etc.

Action Entity settings

The next settings that will be displayed will depend on the Action Type selected above.

<u>AREA or AREA LIST</u>		
Area or Area List to control.		Select the Area or Area List to be controlled by this Action.
Control Type.	Normal Defer Twenty-four Hour Cancel Exit Delay	Select the type of control to be performed. Normal Arm/Disarm Start Defer Arming Timer Arm Disarm 24 Hour (Tamper) part of Area Cancel Exit Delay timer and Arm
When Asserted / When De-asserted	Nothing Arm Disarm Toggle	“When Asserted” specifies the operation that will be performed on the selected entity when the action is asserted. “When De-asserted” specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. Area or Area List will be Armed. Area or Area List will be Disarmed. Area will change to the opposite state. (NOTE: Not applicable to Area List Control)
<u>AUXILIARY or AUXILIARY LIST</u>		
Auxiliary or Auxiliary List selection.		Select the Auxiliary or Auxiliary List to be controlled by this Action:
Control Type	Normal Timed Only Leave Timer	Select the type of control required for this Auxiliary/Aux List. Auxiliary will be controlled as specified in the Action. If a timer is currently running on the Auxiliary, the timer will be restarted with the new timer value. If a timer is currently running on the Auxiliary, it will not be refreshed.
On Time.		If the Auxiliary action requires an On timer, program the timer value in Hours, Minutes and Seconds. A value of up to 65535 Seconds may be programmed. i.e. 18 Hrs, 12 Mins and 15 Seconds.
Off Time.		If the Auxiliary action requires an Off timer, program the timer value in Hours, Minutes and Seconds. Value setting as above.
Auxiliary Action options	Delay On Delay Off Update Dynamic Only	If required, select one or more of the required Auxiliary Action options. Delay On instead of Timed On. Delay Off instead of Timed Off. Update dynamic only. Changes the internal state, but does not change the real state of the output.

When Asserted / When De-asserted	Nothing Turn On Turn Off Toggle	“When Asserted” specifies the operation that will be performed on the selected entity when the action is asserted. “When De-asserted” specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. Auxiliary or Aux List will be turned On. Auxiliary or Aux List will be turned Off. Auxiliary will change to the opposite state. (NOTE: Not applicable to Auxiliary List Control)
<u>DOOR or DOOR LIST</u>		
Door or Door List selection.		Select the Door or Door List to be controlled by this Action:
Unlock time		If the Door or Door List is required to Unlock for a specific period of time, program the timer value in Hours, Minutes and Seconds. A value of up to 65535 Seconds may be programmed. i.e. 18 Hrs, 12 Mins and 15 Seconds.
When Asserted / When De-asserted	Nothing Lock Unlock Toggle	“When Asserted” specifies the operation that will be performed on the selected entity when the action is asserted. “When De-asserted” specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. Door or Door List will be Locked. Door or Door List will be Unlocked. Door will change to the opposite state. (NOTE: Not applicable to Door List Control)
<u>FLOOR (LIST) and LIFT CAR (LIST)</u>		
Floor or Floor List		Select the Floor or Floor List to be controlled by this Action.
Lift Car or Lift Car List		Select the Lift Car or Lift Car List to be controlled by this Action.
Cancel Button Timer		Select this option if this action is to cancel any Floor selection button timers currently running for this Floor.
Floor Time		If the Floor or Floor List is required in Free Access for a specific period of time, program the timer value in Minutes and Seconds. A value of up to ??? may be programmed.

When Asserted / When De-asserted	Nothing Secure Unsecure Toggle	“When Asserted” specifies the operation that will be performed on the selected entity when the action is asserted. “When De-asserted” specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. Floor or Floor List for the nominated Lift Car or Lift Car List will be Secured. Floor or Floor List for the nominated Lift Car or Lift Car List will be put into Free Access. Floor for nominated Lift Car will change to the opposite state. (NOTE: Not applicable to Floor List or Lift Car List Control)
<u>TRIGGER INPUT</u>		
Input to trigger		Select the Input to be controlled by this Action.
State to trigger	Alarm Mask Orientation Fault Range Tamper Low Tamper High Tamper Zone Self-test Failure Low Battery Encryption failure Poll failure Spare Soaking Soak Test Fail Isolate	Select the Input state to be triggered. The “Alarm” state will normally be chosen.
Update State	False (unchecked) True (Checked)	Selects whether the Action will cause the nominated state selected above to be a momentary or permanent change. When the action is executed the Input will only have an “edge” generated for the Input and will then return to the previous state. The Input will remain in the selected state after the Action has been executed. i.e. An “edge” is generated for the Input and then the Input is left in the nominated State.
When Asserted / When De-asserted	Nothing Trigger Restore Toggle	“When Asserted” specifies the operation that will be performed on the selected entity when the action is asserted. “When De-asserted” specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. The nominated Input State will be Triggered. The nominated Input State will be Restored. The nominated Input State will change to the opposite state.

<u>SET AREA USER IS IN (User Location)</u>		This action is used to put a User in a particular Area. This will also cause Area User counts to be updated (i.e. Area User count for the Area the User is in will be decremented and Area User count for the Area the User is put in, will be incremented. As a result, one or more Area User count actions may be invoked if required.
User.		Select the User to whom the nominated Area will be assigned.
Don't update Area User Counts		Enable this option if you do not want the Area User Count to be incremented/decremented when the User location is altered.
Area.		Select the Area to be assigned to the User by this Action.
When Asserted / When De-asserted	Nothing Set Unset Toggle	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. The nominated Area will be set as the Area the User is in. No action. No action.
<u>SET AREA USER COUNT (Number of Users in Area)</u>		This action is used to set the number of Users in Area to a number. Area User count action will not be tested.
Area.		Select the Area to be adjusted by this Action.
User Count		Enter the value that the Area Count will be set to when the Action is triggered. The value is programmable from 0-99999999.
When Asserted / When De-asserted	Nothing Set Unset Toggle	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. User Count will be set to the programmed value for the nominated Area. No action. No action.
<u>SET INPUT COUNTERS</u>		
Input.		Select the Input that will have its Count adjusted by this Action.
Count		Enter the Count Value required. The selected Input will have its count adjusted to this value when the Action is triggered.

When Asserted / When De-asserted	Nothing Set Unset Toggle	“When Asserted” specifies the operation that will be performed on the selected entity when the action is asserted. “When De-asserted” specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. Count will be set to the programmed value for the nominated Input. No action. No action.
<u>SIREN CONTROL</u>		
LAN Module		Select the Module for which Sirens will be controlled by this Action.
Time		Enter a Siren Time in Hours, Minutes and Seconds. Determines how long the siren will stay active when the Action is triggered. A time of up to 1 Hr, 49 Min and 13 Seconds may be set.
Siren Tone	None Bell Sweep Fire Evacuation Chirp: Arm Fail Chirp: Arm Success Exit Delay Warning	Select the Siren Tone to be used for this Action. None Bell Chime tone Intruder Alarm Sweep tone Fire tone Evacuation tone Chirp: Fail. Mid frequency tone followed by LOW frequency tone. Intended to indicate that an attempted operation failed. Chirp: Success. Mid frequency tone followed by HIGH frequency tone. Intended to indicate that an attempted operation succeeded. Exit Delay Warning Different siren tones have different priorities as follows: -
Siren Options	Sound Internal Siren Sound External Siren Override Priority	Siren options allow you to select which Sirens will be triggered and the Siren tone priority. The Module’s Internal Siren output will be triggered. The Module’s External Siren output will be triggered. If this option is enabled, and the nominated Siren is already running, the Siren tone selected for this Siren Action will override the Siren tone currently sounding, regardless of the Siren tone priority. If this option is not enabled, then the highest priority Siren tone will sound.

When Asserted / When De-asserted	Nothing Turn On Turn Off Toggle	“When Asserted” specifies the operation that will be performed on the selected entity when the action is asserted. “When De-asserted” specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. Siren will be turned On. Siren will be turned Off. Siren will change to the opposite state. Note that this option only applies to continuous Siren tones and will have no effect on the “Chirp” Siren tone types.
<u>SET TIMER VARIABLE</u>		
Timer		Select the General Timer that will be adjusted by this Action.
Time		Enter a Timer period in Days, Hours, Minutes and Seconds. A time of up to 49 days may be set.
When Asserted / When De-asserted	Nothing Set Unset Toggle	“When Asserted” specifies the operation that will be performed on the selected entity when the action is asserted. “When De-asserted” specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. The General Timer period will be set to the programmed value. Not applicable to Timers. Not applicable to Timers.
<u>SET GENERAL VARIABLE</u>		
General Variable		Select the General Variable that will be controlled by this Action.
Use Entity	False (Not checked) True (Checked)	Select whether the Value or Entity will be used for this Action. Use the programmed “Value” for this Action. Use the selected “Entity” for this Action.
Value		If “Use Entity” is set to “False”, the selected General Variable is set to this value.
Entity		If “Use Entity” is set to “True”, select the Entity that will be evaluated to get its value. The selected General Variable is set to whatever numerical value the entity equates to. Entities currently supported in this option are: Input – Input States Input – Input Count Input – Analogue Value Auxiliary – Analogue Value General Variable Value.

When Asserted / When De-asserted	Nothing Set Unset Toggle	“When Asserted” specifies the operation that will be performed on the selected entity when the action is asserted. “When De-asserted” specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. General Variable will be set to the value of the constant value or entity as selected above. Not applicable to General Variable. Not applicable to General Variable.
<u>CONTROL AIR-CONDITIONING</u>		
Air Conditioner		Select the Air Conditioner to be controlled by this Action.
Mode	Off Heat Cool Ventilate HeatPump	Select the Mode of operation to be applied.
Delay Time		Program the Delay timer. Enter a Timer period in Days, Hours, Minutes and Seconds. A time of up to ??? may be set.
Running Time		Program the Running Time. Enter a Timer period in Days, Hours, Minutes and Seconds. A time of up to ??? may be set.
When Asserted / When De-asserted	Nothing Turn On Turn Off Toggle	“When Asserted” specifies the operation that will be performed on the selected entity when the action is asserted. “When De-asserted” specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. Air Conditioner will be turned On. (After the Delay Time, if programmed) Air Conditioner will be turned Off. (After the Delay Time, if programmed) Air Conditioner will change to the opposite state.
<u>MACRO CONTROL</u>		
Macro		Select the Macro to be controlled by this Action.

When Asserted / When De-asserted	Nothing Start Stop Toggle	“When Asserted” specifies the operation that will be performed on the selected entity when the action is asserted. “When De-asserted” specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. The Macro will be Started. The Macro will be Stopped. The Macro will be toggled. i.e. Started if currently stopped, or stopped if currently running.
<u>ISOLATE / SOAK TEST AN INPUT</u>		
Input		Select the Input to be Isolated or Soak Tested by this Action.
Sticky Isolate		Enable this option if the Input is <u>not</u> to be De-Isolated by Area Off. (Isolated Inputs are normally automatically de-isolated when the Area is turned off, this option prevents auto de-isolate)
Mode	Isolate Mode Soak Mode	Selects whether the Input is to be Isolated, or put in the Soak Test state. The Input will be Isolated. The Input will be set to the Soak Test state.
When Asserted / When De-asserted	Nothing Isolate De-isolate Toggle	“When Asserted” specifies the operation that will be performed on the selected entity when the action is asserted. “When De-asserted” specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. The Input will be Isolated or set to Soak Test. The Input will be De-isolated or removed from Soak Test. The Input will be changed to the opposite state relevant to the Mode selected above.
<u>COMMS TASK CONTROL</u>		
Comms Task		Select the Comms Task to be controlled by this Action.
State	Normal Restart Update All	Select the operation to perform when the Action is triggered.
When Asserted / When De-asserted	Nothing Activate Deactivate Toggle	“When Asserted” specifies the operation that will be performed on the selected entity when the action is asserted. “When De-asserted” specifies the operation that will be performed on the selected entity when the action is De-asserted. No action.

<u>GRANT AMNESTY</u>		
Select Controller		Select the Controller to provide Anti-passback Amnesty for.
When Asserted / When De-asserted	Nothing Grant Amnesty Deny Amnesty Toggle	“When Asserted” specifies the operation that will be performed on the selected entity when the action is asserted. “When De-asserted” specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. Anti-passback Amnesty will be granted for all Users on this Controller. i.e. Location for all Users will be reset to “No Area”. No action will take place. Not applicable to Amnesty.
<u>SET AIR-CONDITIONER TEMPERATURE</u>		
Select Air-conditioner		Select the Air-conditioning Unit to control.
Unit		Enter the Air-conditioning Unit number.
Zone		Enter the Zone number to adjust.
Temperature		Enter the temperature that you wish the nominated Zone to be set to.
When Asserted / When De-asserted	Nothing Turn On Turn Off Toggle	“When Asserted” specifies the operation that will be performed on the selected entity when the action is asserted. “When De-asserted” specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. Set the nominated Air-Conditioner Zone to the programmed temperature. ? Not applicable to Set AirCon Temperature.

Users and Permissions

Entity/Feature	Description
User Codes	Edit User name, credentials, options and permissions.
Permission Groups (User Groups)	Edit User Group name, options and permissions.
Lists	Edit the names and members of Lists. Available Lists are: • Area Lists • Door Lists • Telephone Number Lists • Floor Lists • Lift Car Lists • Auxiliary Lists
Groups	Edit the names, options and permissions of Groups. Available Groups are: • Menu Groups • Process Groups • Interlock Groups
Backup Cards	Not yet implemented.
RF Remotes	Register or De-register an RF Remote, set its status and associate it with an RF Remote Template and a User.
Card Templates	Edit Card Templates. A Card Template is assigned to each User with a card credential to define how their card will be processed.
RF Remote (Fob) Templates	Edit RF Remote Fob Templates. An RF Remote Template is assigned to each RF Remote to define how the Fob will operate.
Apartments	Edit Apartment settings. Apartments allow an Intercom unit to be linked to an access controlled Floor.

User Codes

Feature	Option	Description
User Codes		Select the User you wish to edit.
User Name		Program a text name for the User of up to 32 characters in length.
Security PIN		The Security PIN is the primary PIN code for a User, and is used to logon to Terminals and perform keypad security operations. If a Qualify PIN is not programmed (see below), the Security PIN is also used in the User's Access Control operations. Enter a PIN Code of up to 8 digits. The Security PIN MUST be unique for every User.

Qualify PIN		The Qualify PIN, if programmed, is the PIN Code that will be used in User Access Control operations. i.e. When the Door Credential Mode is “PIN only”, “Card & PIN” or “Card OR PIN”. If a Qualify PIN is not programmed, the User’s Security PIN is used for these operations. The Qualify PIN can never be used to logon to a Terminal. Enter a PIN Code of up to 8 digits. The Qualify PIN does NOT have to be unique for every User.
Enter Card Number		If the User’s Card data is assigned via the “Enter Card Number” method, the following two options must be programmed.
	Card Template	Select the Card Template relevant to this User.
	Card Data	The raw card data for the User’s Card may be entered in these fields in HEX format. Up to 24 Hexadecimal characters may be entered.
RF Remotes	Remote Template	Select the Fob Template that defines the Fob operations and permissions relevant to the User being programmed.
	Remote Data (ID)	Allows the User’s RF Fob ID to be viewed and/or edited.
	Status	Shows the current status of the RF Remote.
Primary Permission Group (Qualify Group)		Select the Permission Group that defines the operations and permissions relevant to the User being programmed. Permission Groups (Qualify Groups) are programmed separately.
Extra User Permissions		Up to 8 additional User Permissions may be assigned to the User to define operations and permissions for the User. This may not be necessary if all the operations and permissions required for this User have already been defined via the “Primary Permission Group”. Extra User Permission Groups can be assigned in addition to, or in place of, the User’s Primary Permission Group. e.g. To define the Menu Group, Area List, Door List, User Operations, etc, allowed.
	What When	Defines the entity for this User Permission. e.g. Door List, Menu Group, etc. Defines when the entity is valid for this User Permission. e.g. Time Period, Area state, etc. <i>See “Permission Programming” for details of how to program this User option.</i>

User Options	Cancel on Card access. Cancel on PIN Logon. Handicapped User. Duress Code. User Cancelled. No Greeting Permanent Cache. Default Floor Start Date/Time Expiry Date/Time	Enable/Disable the general options for this User. User's permissions will be cancelled after next card use. User's permissions will be cancelled after next PIN use. Longer unlock times etc, if programmed, will automatically be invoked. The Duress System Input will be triggered on the Module where this User PIN and/or Card is used. User is currently cancelled. No security or access operations will be allowed. Greetings will not be displayed for this User when logging on to an LCD Terminal. This User will be stored permanently in the Card Cache on Reader Modules for access when the Module is offline. Sets the default Floor that will optionally be sent to the Elevator Management System on door access. If programmed, the "User Cancelled" option will be cleared at the designated Date and Time. If programmed, the "User Cancelled" option will be enabled at the designated Date and Time.
Lockout Options	Lockout Enabled. Lockout control	Programs options relating to the EN50131 User Lockout feature. Causes this User to be locked out when the Control Module "Enable Lockout" mode is set. Enables this User to allow locked out User permission to logon with a PIN entry.
User Tenancy Area		Area to be optionally armed and/or disarmed on Door access and/or Reader arming, instead of the Area/s assigned to the inside/outside of the Door.

Permission Groups

Entity/Feature	Option	Description
Permission Groups		Select the User Permission Group you wish to edit.
Name		Program a name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Permissions		Up to 16 Permissions may be assigned to the Permission Group to define operations and permissions for this Group.
Permissions 1 to 16	What When	Defines the entity for this User Permission. e.g. Door List, Menu Group, etc. Defines when the entity is valid for this User Permission. e.g. Time Period, Area state, etc. <i>See "Permission Programming" for details of how to program this option.</i>

Offline Permission		Not yet implemented. Not supported in Concept Access Modules. Defines the Permissions for operations performed at Intelligent Access Modules when Offline. Parameters of “Offline Permissions” are programmed separately.
--------------------	--	--

Lists

Entity/Feature	Option	Description
Lists	Area Lists Door Lists Telephone Number Lists Floor Lists Lift Car Lists Auxiliary Lists	Edit the names and members of Lists. Lists simplify the programming of other entities such as User Permissions, Permission Groups and Actions by providing pre-programmed groups of the same entity.
AREA LISTS		Select the Area List you wish to edit.
	Area List Name	Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
	Area assignment.	Assign the required Areas to this Area List. Highlight the required Areas in the bottom (Not In List) field and click on the “Add” button to assign them to the List. Once an Area is in the List it will be displayed in the top ((In List) field.
DOOR LISTS		Door Lists are edited in the same manner as Area Lists described above.
TELEPHONE NUMBER LISTS		Select the Telephone Number List you wish to edit.
	Name	Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
	Assign Telephone Numbers	Assign the required Telephone Numbers to the list. Select from the available Telephone Numbers in the “Not In List” field. The Telephone Numbers are programmed separately.
FLOOR LISTS		Floor Lists are edited in the same manner as Area Lists described above.
LIFT CAR LISTS		Lift Car Lists are edited in the same manner as Area Lists described above.
AUXILIARY LISTS		Select the Auxiliary List you wish to edit.
	Name	Program a text name of up to 32 characters in length.
	Assign Auxiliaries	Assign the required Auxiliaries to the list. Select from the available Auxiliaries in the “Not In List” field. Up to 16 Auxiliaries can be assigned to an Auxiliary List.

Groups

Entity/Feature	Option	Description
Groups & Types	Menu Groups Process Groups Interlock Groups	Edit the names, options and permissions of Groups. Group simplify the programming of other entities such as Users, Doors, Input processing and Modules by providing pre-programmed entities that define permissions and operations.

<u>MENU GROUPS</u>		Select the Menu Group you wish to edit.
Name		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Menu Permissions	Area Information Access Isolate Testing Time Miscellaneous Installer/Engineer Service Control Lists Groups Edit Input Counters Edit User Counters RF Remote Full Test suite allowed Alter Any PIN	Defines which Menu options are allowed at a User Terminal for Users with this Menu Group.
Sub Menu Permissions 1	User Codes User Groups Review Date and Time Time Periods Schedules Holidays LCD Messages Card Formats Card Templates Soak	Defines which Sub-Menu options are allowed at a User Terminal for Users with this Menu Group.
Area Control Permissions.	Initiate Defer Isolate on Exit 24 Hour Off Default List Isolate All Sticky Isolate	Define which Area and Zone Isolate operations are allowed. User will initiate a deferred Area Off operation if turning off an Area defined as a “Defer” Area. Unsealed Inputs will automatically be Isolated on Area Arming. User is allowed to turn off the 24-Hour (Tamper) part of an Area. Terminal display will default to Area List control on User logon. User is allowed to Isolate any Input. Not just Inputs in Areas that they have permission for. User is allowed to Sticky Isolate an Input. i.e. The Input will not be automatically de-isolated on Area Off.

Access Control Options	Exit (Leaving) options Outside Area OFF on Egress (Exit) User Area Off on Egress (Exit)	Access Control Leaving (Exit or Egress) options. Defines Area control operations allowed from Access control Exit Readers. Door “Outside” Area will turn Off on egress. Door “Tenancy Area” will turn Off on egress.
	Entry options Inside Area OFF on Ingress (Entry) User Area Off on Ingress (Entry)	Define the Access Control Entering (Entry or Ingress) options. Defines Area control operations allowed from Access control Entry Readers. Door “Inside” Area will turn Off on entry. Door “Tenancy Area” will turn Off on entry.
	General User Credential options. Dual User Provider Dual User Override Anti-Passback Override Dual Credential Override (e.g. Card + PIN Override)	This User can provide a credential to validate another User when “Dual User” access is required. This User will not require another User to validate when Dual User” access is required. This User can override an Anti-passback restriction. This User can override the need for a second credential when the Door has options such as “Card + PIN” enabled.
Advanced Options	Named Action Groups	Named Actions (Predefined Actions) can be grouped together in up to 16 Action Groups. This is done in the Named Action programming. This option allows the Action Groups that are allowed for Users with this Menu Group to be defined. Select which of the 16 Action Groups are allowed.
Remote Control Permissions	Arm Area Disarm Area Arm 24 Hour Part of Area Disarm 24 Hour Part of Area Isolate Control Aux Lock Door Unlock Door Siren control Comms Task control Adjust Count Secure Allowed. Free Access Allowed. Installer Access	Define the Remote Control operations allowed for this Menu Group. Area Arming allowed Area Disarming allowed Arming of 24-Hour (Tamper) part of Area allowed Disarming of 24-Hour (Tamper) part of Area allowed Isolate allowed Auxiliary control allowed Lock Door allowed Unlock Door allowed Siren control allowed Enable/Disable Comms Task control allowed Adjust Counter values allowed Can Set Lift Floor/s to Secure mode. Can Set Lift Floor/s to Free Access mode. Can connect to Panel via Integriti CS (Commissioning Software). E.g. via iModem or USB.

Review Level	Everyone User - Essential User - Standard User - Detailed Installer - Standard Installer - Detailed Inner Range - Debug	Select the Review Level required for Users with this Menu Group. This option determines the amount of detail that will be included in the Review log. Lowest level of detail. Highest level of detail. The Review Level settings in the four default Menu Groups will give a guide to how you might select this setting in any additional Menu Groups programmed.
Review Classifications	Input Area User Communications Isolate Module Siren General Variable Timer Auxiliary Door Rtos Area Timer C info Lift Time Period Holiday Schedule Debug Air-conditioning Area Counters Input Counters RF Device Information	Select the Categories required for Users with this Menu Group. This option determines the types of entities that will be included in the Review log. The Review Classification settings in the four default Menu Groups will give a guide to how you might program these options in any additional Menu Groups programmed.
Message Acknowledge	Acknowledge message. Acknowledge All Messages. Auto Siren Off. Clear EN pins on logon	Select the Message Acknowledge options required. The User is allowed to acknowledge alarm messages in the Areas that they have permission to turn Off. The User is allowed to acknowledge all alarm messages. Sirens sounding in the Areas that the User has permission to turn Off, will be cancelled on User logon. ???
EN: Message Acknowledge Options	Clear UK Lock Clear EN Alarm Clear EN Fault	
Message Acknowledge options	Clear Annunciate	

<u>PROCESS GROUPS</u>		Select the Process Group you wish to edit. Process Groups define how Inputs of the same type are to be processed. A Process Group is assigned to each Zone or System Input when it is placed in an Area. Integriti allows extremely flexible Input processing by allowing a different Process Group to be assigned for each Area that a Zone is in. e.g. The same movement detector can provide Intruder alarm monitoring in one Area, while also providing timed lighting control in another Area.
Name		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
States to process.	<u>EOL Input States</u> Alarm Mask Orient Fault Range Tamper Low Tamper High Tamper <u>Logical Input States</u> Zone Self-Test Fail Battery Crypto Fail Poll Fail spare Soaking Soak Test Fail Isolate	EOL Input States. Most devices only support one or more of the physical states; Alarm, Tamper Low, Tamper High and Tamper. Do not select other states for monitoring unless you understand how the relevant EOL scheme operates for those states. Logical Input States. Most devices only require the Zone Self-Test Fail and/or Isolate states to be processed. Do not select other states for monitoring unless you understand how the Logical Input States scheme operates.
Processing.	Entry Zone. Exit Zone. Primary Entry Zone. Pulse Count Zone. One Pulse Count only. No 24 Hour if Armed. Process 24 Hour. 2nd Stage Arm EN Ack requires Installer	Inputs will have Entry Delay applied on selected states. Inputs will have Exit Delay applied on selected states. Inputs can start the Entry Timer. Inputs will have Pulse Count logic applied. Inputs can only contribute one pulse per Input to the Pulse Count. 24-Hour Input states will not be processed while Area armed. The EOL "Alarm" states will be processed as 24-Hour states. Inputs are processed the same, regardless of the On/Off state of the Area.

Messages. (Terminal message options)	States to generate Terminal messages <u>EOL Input States</u> Alarm Mask Orient Fault Range Tamper Low Tamper High Tamper <u>Logical Input States</u> Zone Self-Test Fail Battery Crypto Fail Poll Fail spare Soaking Soak Test Fail Isolate	Define the EOL Input States to generate Terminal messages. Options are the same as “Input States to process” above. Define the Logical Input States to generate Terminal messages. NOTE: Do not edit these options unless you understand how the Input States scheme operates.
	Terminal Message Categories.	Select one or more of the Message Category/s to allow messages from this Process Group to be sent to User Terminals with the corresponding Message Category options enabled. Up to 8 Message Categories may be utilized. e.g. 1) To send all messages to all Terminals simply assign Category 1 in all Process Groups, and Category 1 in all Terminals. 2) To ensure Intruder and Holdup alarm messages are not sent to Terminals in Public access areas, only assign Category 2 to Process Groups for these types of alarms, then enable Category 2 for Terminals in secure Areas, but disable Category 2 for Terminals in public Areas.
Communications Options. (Reporting)	<u>EOL Input States</u> Alarm Mask Orient Fault Range Tamper Low Tamper High Tamper <u>Logical Input States</u> Zone Self-Test Fail Battery Crypto Fail Poll Fail spare Soaking Soak Test Fail Isolate	Define the EOL Input States to report. Options are the same as “Input States to process” above. Define the Logical Input States to report. Options are the same as “Input States to process” above. NOTE: Do not edit these options unless you understand how the Input States scheme operates.

	Comms Task Groups	Option to allow Input event reporting to be filtered based on the type of Input. Up to 16 separate Comms Task reporting Groups can be established. If one or more Groups are enabled in these options, the Input events will only be reported by Comms Tasks that have: - At least one matching Comms Task Group enabled, - Or - No Comms Task Groups enabled. If no groups are enabled in these options, the Input events can be reported by any Comms Task, regardless of how the Comms Task Group options have been set in the Comms Task Programming.
	Reporting options. Report Entry. Report Exit. No Restore. Delay Report.	Select the required general reporting options. Transmit Alarm events during Entry. Transmit Alarm events during Exit. Don't report Input state Restores. Delay Reporting of events by the Comms Task Delay Report Time.
	Swinger Shutdown Count	Maximum number of reports that can be sent on an Input before the Input is Isolated.
	Swinger Shutdown Input States. <u>EOL Input States</u> Alarm Mask Orient Fault Range Tamper Low Tamper High Tamper <u>Logical Input States</u> Zone Self-Test Fail Battery Crypto Fail Poll Fail spare Soaking Soak Test Fail Isolate	Define the Input States, that if reported, will be used in the Swinger Shutdown count. Options are the same as "Input States to process" above. NOTE: Do not edit these options unless you understand how the Input States scheme operates.
	Contact ID Message Type (Event Code)	Enter the Contact ID Event Code to be used for this Process Group. If left at "000", the Contact ID Event Code assigned to the individual Input (if programmed), or a default Contact ID Event Code, will be used. An appropriate default Contact ID Event Code is assigned to each of the pre-programmed Process Groups provided. <i>See the following table for details.</i>

	EN Pin state. None Fire Panic Intruder Fault Power Jam Battery Mask Soak Primary ATS Secondary ATS Tamper Soaking Spare Spare	Enter the EN Pin state to be used to identify the alarm type from this Process Group. None (Pin 0) Fire (Pin 1) Panic (Pin 2) Intruder (Pin 3) Fault (Pin 4) Power (Pin 5) RF Transmitter Jam (Pin 6) Battery (Pin 7) Mask (Pin 8) Soak Fail (Pin 9) Primary Alarm Transmission System (Pin 10) Secondary Alarm Transmission System (Pin 11) Tamper (Pin 12) Soaking (Pin 13) Spare (Pin 14) Spare (Pin 15)
	4+2 Reporting format Event Code.	Enter the 4+2 Code to be used to identify the alarm type from this Process Group when reporting in 4+2 Dialler format.
Siren Programming	None Bell Sweep Fire Evacuation Chirp: Arm Fail Chirp: Arm Success Exit Delay Warning	Select the Siren Tone to be used for Alarms for this Process Group. Select the Siren Tone to be used for this Action. None Bell Chime tone Intruder Alarm Sweep tone Fire tone Evacuation tone Chirp: Fail. Mid frequency tone followed by LOW frequency tone. Intended to indicate that an attempted operation failed. Chirp: Success. Mid frequency tone followed by HIGH frequency tone. Intended to indicate that an attempted operation succeeded. Exit Delay Warning Different siren tones have different priorities as follows: -
	External Siren Input states.	Define the Input States to trigger External Sirens. Options are the same as “Input States to process” above.
	Internal Siren Input states.	Define the Input States to trigger Internal Sirens. Options are the same as “Input States to process” above.
	Siren Options Siren Lockout Siren Refresh	Select the Siren control options required. An Input that triggers the Siren/s will be Isolated at the end of the Siren Time. If an Input triggers the Siren/s while the Sirens are already running, the Siren timer will be re-started.

Action Programming	Action Assert Input states.	Define the Input state/s that will <u>trigger</u> the nominated Area Process Action when asserted. Options are the same as “Input States to process” above. Up to 8 Input Process Actions can be programmed.
	Action De-assert Input states.	Define the Input state/s that will <u>cancel</u> the nominated Area Process Action when de-asserted. Options are the same as “Input States to process” above. Up to 8 Input Process Actions can be programmed.

Integriti Default Process Group Contact ID Event Codes and typical applications.

	Default Process Group	Default CID Event	Input Example
1	Intruder/Burglary	130	Internal intruder detector
2	Entry-Exit/Burg Delayed	130	Internal intruder detector in Entry-Exit path
3	Intr/Burg Primary	130	Intruder detector at point of entry
4	Silent Alarm	150	Plant alarm with off-site reporting
5	Local Alarm		Plant alarm with local audible/visual annunciation only
6	Local Silent		Plant alarm with Terminal message only
7	Fire	110	Smoke or Heat-rise detector
8	Duress	121	Duress device or Keypad Duress
9	Panic	123	Panic device or Terminal Panic
10	Emergency	100	Evacuation device
11	Automation		Lighting and HVAC control
12	Log & Report Only	300	Memory Fault
13	Log Only		
14	Tamper	145	Cabinet Tamper Siren Tamper LAN Power Supply Auxiliary Tamper
15	LAN Fault	143	LAN Comms Fail LAN Unsecured
16	AC Fail	301	AC Fail
17	Battery Problem	302	Low Battery Battery Test Fail Battery Fail
18	Power Supply Fault	312	Fuse Fail Low Volts Detector Over-current Battery Over-current Over Volts PS Slave Fail
19	Comms Problem	350	Unibus Problem Comms Backup Triggered Comms Fail Phone Line
20	RF Transmitter Fault	381	RF Transmitter Timeout RF Transmitter Low Battery RF Transmitter Poll Fail
21	RF Jam	344	RF Transmitter Jam
22	Access Alarm	423	Door Forced Lock Tamper
23	Access Silent	426	DOTL
24	Access Local		Too Many Tries Illegal Card
25	Time Report	602	Triggers Periodic Test Report

<u>INTERLOCK GROUPS</u>		Select the Interlock Group you wish to edit.
Name.		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Interlock Entities	What When	Program or Edit the “Interlocked Entities” for this Interlock Group. e.g. To define the Door List, Area, etc., to be applied in the Interlock logic. Defines the entity for this Interlock Entity. e.g. Door List, Menu Group, Input, etc. Defines when the entity is valid for this Interlock Entity. e.g. Time Period, Area state, etc. Up to 16 Interlock Entities can be assigned to an Interlock Group. <i>See “Permission Programming” for details of how to program this option.</i>

RF Remotes

Entity/Feature	Option	Description
Name		Program a name of up to 32 characters for this RF Remote. The name may include the User’s name and/or the purpose of the Remote.
Credential	Remote Data	Allows an RF Remote ID to be viewed and/or manually entered.
	Remote Template	Assign an appropriate RF Remote Template to this Remote to define the operations.
Association	Associated User	Select the User to whom this RF Remote will be issued.
Miscellaneous	Status Active Inactive – Lost Inactive - Suspended	Set the status for this RF Remote.

RF Remote Templates

Entity/Feature	Option	Description
Name		Program a name of up to 32 characters for this RF Remote Template. The name may include the main purpose and/or functionality offered by the template.

Button Definitions	Actions	Program the Action for each button to be used. Depending on the Remote Model, up to 4 Button Actions may be programmed. <i>See Table Below.</i>
	Areas	Select one or two Areas to be controlled. Depending on the Remote Model, up to 2 Areas or Area Lists may be selected. <i>See Table Below.</i>
	Inputs	Select one or two Inputs to be controlled. Depending on the Remote Model, up to 2 Inputs may be selected. <i>See Table Below.</i>
Options	Needs 6 Digits Needs PIN for Programming Needs PIN for Area On/Off	If PIN Code operation is selected, this option forces a requirement for PIN Codes to be 6 digits long. ??? PIN Code is required for Area On/Off operations. Only relevant to Paradox REM3.

RF Remote operations supported

Brand/ Model	Button Actions				Areas		Inputs	
	1	2	3	4	1	2	1	2
Paradox REM1	On	=>			Y			
Paradox REM2	●	●●			Y			
Paradox REM3	PGM1	PGM2	PGM3	PGM4	1 & 7	2 & 8		
Paradox REM?								
Visonic MCT-231		●						
Visonic MCT-234	🏠	Unlock	Lock	*				

Card Templates

Entity/Feature	Option	Description
Card Template		Select the Card Template to program. Card Templates enhance User programming by combining the Card Format and Site Code in a single entity.
Name		Program a name of up to 32 characters for this Card Template. The name may include the format of the cards and/or the tenancy of the Users.
Format		Select the Card Format for this Template. <i>See Reader Module programming for a list of pre-defined Card Formats.</i>

Site Code		Enter the Site Code for this Template. The Site Code can be entered in Decimal or Hexadecimal format. When the Site Code is entered in one field, the other field will automatically be populated with the equivalent number in the alternate format.
-----------	--	--

Apartments

Feature	Option	Description
Apartment		Select the Apartment you wish to edit. Apartments allow an Integriti Floor to be associated with an Intercom Unit and Floor. This feature operates in conjunction with the “Intercom” Comms Task format to provide sophisticated Intercom access control integration.
Name		Program a text name of up to 32 characters in length. The name may include the Apartment number and/or Floor details.
Settings	Floor	Select the Floor to be associated with this Apartment.
	Intercom System Floor	Enter the Intercom system Floor number to be associated with this Apartment.
	Intercom System Unit	Enter the Intercom system Unit number to be associated with this Apartment.

Times

Entity/Feature	Option	Description
Times		The various Times entities provide all the settings and programming options relating to Time/Date, Time Periods, Schedules and programmable LCD Terminal messages.
Time and Date		Set the current Time and Date.
Time Periods		Edit Time Period name, Time/Day parameters and options.
Schedules		Edit Schedule name, Start/Stop Date & time, Days of week and options.
Holidays		Edit Holiday name, Start/Stop Date & Time and options.
LCD Messages		Edit the LCD message name, control entity and message text.

Time and Date

Entity/Feature	Option	Description
Time and Date		The Controller Time and Date is normally synchronised with the software when a connection between the software and the Controller is established. The Controller Time and Date can also be synchronised periodically by programming a Scheduled Task to define when, and how often, the Date and Time will be synchronised. There is currently no means of manually manipulating the Controller's Real-time Clock from the Software. If the Controller's Real-time Clock needs to be changed to a different time for testing and commissioning purposes, this must be done at an LCD Terminal via MENU, 5, 1. If there is a Scheduled Task programmed to synchronise the Controller time, you may wish to disable it while performing the testing.

Time Periods

Entity/Feature	Option	Description
Time Periods		Select the Time Period you wish to edit.
Name		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Options	Defined in UTC Time	Program the options for this Time Period. Time Period is defined in Greenwich Mean Time (GMT). i.e. Coordinated Universal Time (UTC).

Start and End times.	Start Time End Time	Program the Start and End time for the Period. Up to 4 separate Periods can be programmed.
Period Days of Week.	Sunday Monday Tuesday Wednesday Thursday Friday Saturday Ignore Holidays	Assign the Days of Week to be used in the Period. The Period will only be Valid on the days specified. Select “Ignore Holidays” if the Time Period will not be made invalid by Holidays. Up to 4 separate Periods can be programmed.
Holidays		Assign the Holidays that will be obeyed by this Time Period. Up to ?? Holidays can be defined.

Schedules

Entity/Feature	Option	Description
Schedules		Select the Schedule you wish to edit.
Name		Program a name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Schedule Options	UTC Time	Program the options for this Schedule. Schedule is defined in Greenwich Mean Time (GMT). i.e. Coordinated Universal Time (UTC).
Start Date/Time		Program the Start Date and Time for this Schedule. Enter the current Time and Date in the format; DD/MM/YY – hh:mm Where: DD = Day of month MM = Month YY = Year hh = Hours in 24Hour format mm = minutes
Stop Date/Time		Program the Stop Date and Time for this Schedule. The format is the same as Start Date/Time above.
Days of Week	Sunday Monday Tuesday Wednesday Thursday Friday Saturday	Program the Days of Week for this Schedule. Options are the same as the Days of Week options in Time Period programming, but without the Holidays option.

Recurrence Frequency		Select the recurrence frequency for this Schedule. Selecting a repeat frequency causes the nominated value in the Time/Date setting to be ignored. e.g. If “Daily” is selected then the day part of the date setting will be ignored. This allows the Schedule to repeat in the nominated period within the limits of the other values in the Date/Time setting. e.g. If “Daily” is selected, then the Schedule will repeat at the same time each day in the nominated Month and Year. Never Hourly Daily Weekly Monthly Yearly Weekday Of Month Single shot at the programmed Start/Stop Date & Time. Repeat Hourly. Repeat Daily. Repeat Weekly. Repeat Monthly. Repeat Yearly. Repeat on the same day each month.
----------------------	--	--

Holidays

Entity/Feature	Option	Description
Holidays		Select the Holiday you wish to edit.
Holiday Name		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Start Date/Time		Program the Start Date and Time for this Holiday. Enter the current Time and Date in the format; DD/MM/YY – hh:mm Where: DD = Day of month MM = Month YY = Year hh = Hours in 24Hour format mm = minutes
End Date/Time		Program the Stop Date and Time for this Holiday. The format is the same as Start Date/Time above.
Holiday Options	Recur Annually Use UTC Time	Program the options for this Holiday. Repeat this Holiday Annually. This option is used for holidays that recur on the same date every year. If this option is enabled, the Year value in the Start and Stop settings is ignored. Holiday is defined in Greenwich Mean Time (GMT). i.e. Coordinated Universal Time (UTC).

LCD Messages

Entity/Feature	Option	Description
LCD Messages		Select the LCD Message you wish to edit.

Name		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Message Text		Program the message text. Up to 160 characters may be entered for the message.
Select Qualifier Entity		Defines the entity that will be used to cause the LCD Message to be valid. e.g. A Time Period, Area Status, Schedule, etc.
Qualifier Options	Invert Qualifier	Inverts the logic of the Message Qualifier. i.e. The message text will be displayed when the Qualifier is Invalid.

Installer

Entity/Feature	Option	Description
Installer		The programming options listed in this section of the manual cover the settings and programming options relating to installation, commissioning and operation of the system.
Inputs		Program/Edit the Input parameters.
Areas		Program/Edit the Area parameters.
Modules	LCD Terminal Expander 2-Door Reader Module Integriti Graphic Terminal RF Expander Power Supply Module Integriti 4-Door Access Module Analogue Module Fob and Zone Registration Control Module C3K Intelligent 4 Door Controller	Program/Edit the Module parameters. LCD Terminal Expander. Integriti Zone Expander Modules and Legacy Concept 3000 Zone Expander Modules Integriti 2-Door Reader Module and Legacy Concept 3000 ½ Door Reader Modules. Integriti Graphic Terminal Legacy Concept 3000 RF Expander Modules Legacy Concept 3000 LAN Power Supply Module (Not yet implemented) Legacy Concept 3000 Analogue Modules. RF Expander Remote Fob and Zone Registration Menu
Communications	Integriti Monitor Dialler GSM Automation EMS Securitel Intercom Sky Tunnel	Program/Edit the Communications parameters.
System	Memory Auxiliaries EOL Configurations	Program/Edit the System configuration and system-wide operations. “Default 1” is currently the only Memory configuration supported. Allows basic Auxiliary parameters to be defined for each Auxiliary. Allows EOL scheme parameters to be viewed and edited. CAUTION! Do not edit parameters or options in this menu unless you fully understand the ramifications of the changes. Changing settings for an EOL scheme will affect the operation of all Inputs in the System that use that scheme. Selection of the EOL scheme to be used on specific banks of Inputs is done in the “Modules” Menu (MENU, 7, 2) and NOT in this Menu.

Access Control	Entity Types and Groups Door Types Qualified Door Types Lift Types Qualified Lift Types Lift Groups	Allows the various Entity Types and Groups related to Access Control operations to be programmed and edited.
	Access Control Entities Card Formats Doors Lifts Floors	Allows the various Entities related to Access Control operations to be programmed and edited.
Automation	Named Actions Macros Air conditioners Comparisons Compound Entities General Variables General Timers Calibrations	Allows the various Entities related to Automation operations to be programmed and edited.

Input Programming

Entity/Feature	Option	Description
Find Input		Select Input to program
Input Name		Program a text name of up to 32 characters in length. This feature can be used to describe the type, location and/or purpose of the Input.
Zone Type	Normal Analogue Count Up Count Down Previous Input Count Up Previous Input Count Down	Select Zone Type. Normal Digital EOL Zone Input. Analogue Zone Input. Event Counter Input, counting up. Event Counter Input, counting down. Event Counter Input, contributing an up count to the previous Zone Input ID. Event Counter Input, contributing a down count to the previous Zone Input ID.
Zone Alarm Action		The Zone Action allows a Zone Input to be programmed to provide direct control of another entity. Once the required Entity is selected, the options relevant to the control of that Entity type will be displayed.
Input Options	Summary Zone. Ignore physical Input. Swap Alarm and Seal No test on Exit. Auto Isolate on exit. Zone Self Test enabled. Don't log to Review. Isolate all only.	Zone Input Options. This Zone will be included in the overall Input summary. Ignore the physical Zone state. Used when the Zone is only to be triggered by an Action or similar operation. Swap the Alarm and Seal states. For Normally Open alarm contacts. The system will not check that this zone is sealed when arming an Area to which it is assigned. E.g. Perimeter Door or Barrier that is used to exit the premises and must remain open until after arming. Auto Isolate on arming. Auto-isolate will be allowed on the Input if the Input is unsealed when as Area to which it is assigned is being turned On. Zone Self Test enabled. Activity on this Input will not be saved to Review. Only a User with the "Isolate All" permission can isolate this Input.

SIA Type State	None ATAR DDDR DFDR DLDH EMEN ESEJ HAHH IAIR JAUX LTLR NANS NCNR NTNR PAPR RPUX RRUX RXUX TATR UAUH UAUR XTXR YFUX YIYJ YPYQ YTYR YXUX UXUX YAYH	Enter SIA Type State. The default SIA Type will be used. AC Power Fail Illegal Card Door Forced Door Open Too Long LAN Comms Fail Seismic Tamper Holdup Duress Too many PIN tries Phone Line Fault RF Transmitter Fail End-Of-Line Module Tamper End-Of-Line Module Comms Fail Panic Periodic Test Report Power-up Reset Manually triggered Test Report Cabinet Tamper Untyped Zone Alarm Untyped Zone Alarm Transmitter Low Battery Checksum Fail (Memory or Download fault) Over-current Power Supply Trouble Low Battery Service Request Undefined alarm Siren Tamper/Fault
Contact ID Message Number		Program the Contact ID Event Type to be used when reporting Alarms on this Zone. The Event Type is a number between 000 and 999. If left at 000, an appropriate default Contact ID message will be used depending on the Process Group assigned to the Input. <i>See the Tables section for details.</i>
Analogue Calibration Type		Select the Analogue Input calibration parameters. Predefined Calibrations are programmed separately, and once programmed, can then be assigned to relevant Inputs.
Counter Calibration Type		Select the Counter Input calibration parameters. Predefined Calibrations are programmed separately, and once programmed, can then be assigned to relevant Inputs.
Logging frequency		Program a frequency in Hours, Minutes and Seconds, to determine how often the Analogue or Counter value on this Input is saved to Review. 0 = No logging. The logging frequency can be set to a value between 1 Second (most frequent logging frequency) and 18 Hours (the least frequent).

Analogue Hysteresis		Sets the sensitivity to changes in analogue values to trigger an Input analogue value update. NOTE: Used for legacy Concept 3000 Analogue Modules only. For Integriti Expanders, this option is set in the relevant Input programming.
Assign the Input to an Area.	Don't forget to assign your Inputs to at least one Area	Assigning Zones and System Inputs to Areas is performed in Area programming.

Area Programming

Entity/Feature	Option	Description
Find Area		Select the Area you wish to edit.
Area Name		Program a text name of up to 32 characters in length. This feature can be used to describe the location and/or function, etc. of the Area.
Reporting Options	Report Opening. Report Closing. Close at Exit Start. Report Openings after Alarm. Report 24 Hour Open/Close Exclude from General Open/Close	Central Monitoring Station reporting options. Report Opening. Report Closing. Report the closing event at the beginning of the exit delay, instead of at the end. Only report Openings for this Area if an Alarm report has occurred since Closing. Report Open/Close on the 24 Hour (Tamper) part of the Area. Do not include this Area as part of a General Area Open/Close report.
	Client Code	Determines the Account code to be sent when reporting events from this Area. An Account Code (Client Code) may be entered for any Areas where the Account Code needs to be different from the one programmed in the relevant Comms Task. Account Codes are typically provided by the Central Monitoring Station. The number of digits required will depend on the reporting format. Enter a Decimal value between 0 – 65535, or a Hexadecimal value between 0 – FFFF.
Entry / Exit	Entry Delay Timer	Sets the Entry delay period upon triggering an entry zone. Enter a value in Hours / Minutes / Seconds. Maximum value is 1 hr, 49 min, 13 sec.
	Exit Delay Timer	Sets the Exit delay period on Area arming if required. Enter a value in Hours / Minutes / Seconds. Maximum value is 1 hr, 49 min, 13 sec.
Process Alarm Actions (Area Input Actions)		Programs the Actions that will occur when at least one of the Input states specified in the corresponding Process Group Input Action are Asserted and/or De-asserted. Up to 8 Area Input Actions are available. Select an Entity type that will be controlled by the Area Input Process Action. After an entity type is chosen, the additional options relevant to control of that type of entity will be displayed. For an Area Input Process Action to operate, the corresponding Input Action/s must be enabled in the Process Group. Note that some of the default Process Groups have Action 1 and Action 2 already defined for the Alarm state and Tamper state respectively where relevant.

Siren Programming	Siren Modules	Determines what sirens will sound when an Input programmed to activate sirens is triggered. Up to 8 Sirens may be assigned to an Area. Additional Sirens may be assigned via the Siren Action or Area Process Actions if required.
	Siren Time:	Determines the siren activation time for sirens assigned to this Area. Check local regulations for any limits on the length of time that Sirens are allowed to run. Enter a value in Hours, Minutes, Seconds. Maximum value is 1 hr, 49 min, 13 sec.
	Siren Holdoff Time:	Determines the Siren Holdoff time for sirens assigned to this Area. The Siren Holdoff time is the amount of time that Siren activation will be delayed. Enter a value in Hours, Minutes, Seconds. Maximum value is 1 hr, 49 min, 13 sec.
	Internal Siren Mode: No Siren Instant Siren Siren on 2nd Hit Siren on Backup	Determines how the Internal Sirens will work if required. No Internal Sirens. Triggered instantly. Triggered on the 2nd hit on any Input programmed to activate Sirens. Only triggered if the Backup Comms Task has been triggered.
	External Siren Mode No Siren Instant Siren Siren on 2nd Hit Siren on Backup	Determines how the External Sirens will work if required. Options are the same as for Internal Siren Mode above.
	Max Siren Trigger	Determines the number of siren activations that can occur in this area before sirens become disabled. The trigger count applies to one arming cycle. Sirens will automatically be re-enabled when the Area is disarmed.
	Siren Action	You may select another Entity type or additional Siren that will be controlled when the Siren Activates and/or Deactivates. After an entity type is chosen, the additional options relevant to control of that type of entity will be displayed.
User Counting	Count Action	Select Count Action - Select the Entity type that will be controlled when the Counter reaches/exceeds the High Count and/or reaches/drops below the Low Count. After an entity type is chosen, the additional options relevant to control of that type of entity will be displayed.
	User Count High Trigger	Determines the Trigger Count High value for Area User Counting. The Count Action will be asserted if the Count value reaches or goes above this value.
	User Count Low Trigger	Determines the Trigger Count Low value for Area User Counting. The Count Action will be De-asserted if the Count value reaches or goes below this value.

Area State Actions		Programs the Actions that will occur when the corresponding Area state is Asserted and/or De-asserted. After an entity type is chosen, the additional options relevant to control of that type of entity will be displayed. <i>See Action Programming in “Generic Programming Operations” for more details.</i>
	Entry Action	Select Entry Action - Select the Entity type that will be controlled when this Area's Entry Delay Starts / Ends
	Exit Action	Select Exit Action - Select the Entity type that will be controlled when this Area's Exit Delay Starts / Ends
	Close Action	Select Close Action - Select the Entity type that will be controlled when this Area is Armed / Disarmed
	Test Action	Select Test Action - Select the Entity type that will be controlled when this Area Starts / Ends Input testing
	Warn Action	Select Warn Action - Select the Entity type that will be controlled when this Area starts / ends the Defer Arming Warning Timer.
	Isolate Action	Select Isolate Action - Select the Entity type that will be controlled when Inputs in this Area are Isolated / De-isolated.
	Unseal Action	Select Unseal Action - Select the Entity type that will be controlled when Inputs in this Area are Unsealed / Sealed
General Area Options	Test for Users when Arming.	Provides a warning if any Users are considered to still be in the Area when it is about to be armed. This option only applies when the Arming operation is being performed at an LCD Terminal or Colour Graphic Terminal. When an Area is Armed successfully, the number of Users in that Area is set to zero.
	Force Area Pre-Arm Walk Test	If there are any Inputs in the Area that must be tested before the next arming, force a pre-arm walk test when the Area is armed at an LCD or Graphic Terminal.
	Sub Area	Allows a sub Area to be defined. The Sub Area will be controlled by the state of its associated Area. Sub-Area programming allows a one or more Areas to control the state of a common Area. e.g. The common Area (Sub-Area) will disarm when the first Area it is associated with disarms, and will only rearm when all of the Areas it is associated with are armed.
	Defer Area.	Allows this Area to be timed off (deferred) by a User with the appropriate permission settings.
	Defer Time	Determines how long this area will remain Off (Disarmed) when turned off and a Defer timer is triggered. i.e. Timed Off. For this feature to operate, the Area must be defined as a Defer Area and the User or Action that performs the Disarm operation must also have the Defer operation enabled. Enter a value in Hours, Minutes, Seconds. Maximum value is 1 hr, 49 min, 13 sec.

	Max Pulse Count	Determines the number of pulse counts required within the pulse count time to generate an alarm. Enter a value of up to 255.
	Pulse Time	Determines the pulse count time to apply to Inputs that are programmed as Pulse Inputs via their Process Group in this Area. The nominated Pulse Count below, must be reached within the programmed Pulse Time, to trigger an alarm. The Pulse Count Timer starts when the first Pulse Count Input is triggered. If the timer expires, and the Pulse Count is not reached, the Pulse Counter is reset. Enter Pulse Time in Hours, Minutes, Seconds. A value of up to 1 h, 49 m, 13 s can be entered.
	Test Time.	Sets the maximum time for Zone Walk Testing. Enter a value in Hours, Minutes, and Seconds. Maximum value is 1 hr, 49 min, 13 sec.
	Arm Self Test Count	Determines the number of times this Area must be switched ON before a Zone self-test is performed. If left at 0, Zone Self Test is disabled. If set to a non-zero value, then every nominated number of arms, at the end of exit delay, any input that has “Zone self test” enabled and has not had a seal to alarm transition since the last Zone Self-Test will assert the ZST fail state, or de-assert the ZST fail state if it passed. In addition a review message will be saved.
	Re-arm options	The Re-arm options provide a feature whereby the Area can be programmed to automatically re-arm if a specified period of Input inactivity has elapsed.
	Re-arm Time	Program a re-arm time. If there is no Input activity in this Area for the nominated period of time, the Area will re-arm. If left at 0, the Area will never re-arm automatically.
	Re-arm Qualifier	A Re-arm Qualifier may be assigned to the re-arm operation. This entity must be valid for Re-arm to occur. e.g. Another Area must already be On. Additional options may be presented depending on the Qualifier Type selected.
	Invert Re-arm Qualifier.	If enabled, the Re-arm Qualifier must be Invalid for Area Re-arm to occur.
	Battery Test on Area Arm	Forces a short Battery Test on all Batteries in the System on an Area Arming.
	Arm 2 nd Stage Delay	
	Soak Test Time	Program the duration required to Soak test Inputs.

Siren	Exit Tone Entry Tone Arm Problem Tone Arm Fail Tone Arm OK Tone Warn Tone	Select the Siren Tone for any of the Area Siren Trigger options required. Siren Tones are the same as those available in “Sirens” above. Siren tone to sound during Exit Delay period. Siren tone to sound during Entry Delay period. Siren tone to sound if there is a problem during the arming procedure. E.g. Unsealed Zones. Siren tone to sound if the Area failed to Arm. Siren tone to sound when the Area successfully Arms. Siren tone to sound during the Defer Arm warning period.
Verify Options	Confirm	Select this option to enable Alarm Confirmation logic for this Area.
	Verify Group	Enter the Verify Group number for this Area.
	Confirmed Alarm Time	Program the Confirmed Alarm Time in Hours, Minutes and Seconds.
	Confirmed Alarm Options Prevent Lockout this Area allowed Isolate Extended Entry	
Inputs	Area Input assignment.	Select an Input to be assigned to this Area, then select the Process Group that will be used for the Input. Note that an Input can be assigned to a maximum of eight (8) different Areas. Additional pairs of Input and Process Group selections are made for each Area that the Input is assigned to.

Modules

Entity/Feature	Option	Description
Modules		Select the Module type you wish to edit.
	LCD Terminal Touchscreen Terminal Expander 2-Door Reader Module Integriti Graphic Terminal RF Expander Power Supply Module Integriti 4-Door Access Module Analogue Module Control Module C3K Intelligent 4 Door Controller	(Not yet implemented) (Not yet implemented)

LCD Terminal

Entity/Feature	Option	Description
Find LCD Term		Select Record to Alter.
LCD Terminal Name		Program a name of up to 32 characters in length. Use this feature to describe the location and/or purpose of the Module.
General Options	Associated Area	Determines the Associated Area for this LCD Terminal. Used in conjunction with other LCD Terminal options.
	LCD Terminal Options No Keypad Beep. Entry Display. Entry Beep. Exit Display. Exit Beep.	Select the general LCD Terminal options required. No feedback beep when keys are pressed. Show Entry Timer countdown for the associated Area. Beep during entry timer for the associated Area. Show Exit Timer countdown for the associated Area. Beep during exit timer for the associated Area.
	LED Mode. None Area Array	Select the default LED operation for this LCD Terminal. LEDs are controlled by the associated Auxiliary only. LEDs will display Area status by default.
Logged Off Display Options.	Idle Display System Ready System Time Single Area Area Array	This message will be displayed on the LCD whilst logged off. The text "System Ready" is displayed The current system time and date is displayed. The status of the Associated Area is displayed A status array for the Associated Area and the subsequent 7 Areas is displayed.

	Display options Display Alarm Messages. Display Status Messages. Display LCD Messages. Display Input Levels. Display Single Message. Display Area Arm Warning	Select the types of messages that the LCD Terminal is allowed to accept. Area Alarm Messages allowed. Area Alarm Message Categories must also be programmed. Select whether terminal will display System Status messages such as Power Supply, Battery, Communication or LAN Network problems. Select whether terminal will display custom LCD Messages. An LCD Message, if Valid, will override the selected Idle Display. Input Level messages allowed. Terminal will display a Single Message for the Associated Area. (Limited Messages) Restricts the LCD Messages to the Defer Arm Warning (“Area about to turn on”) and LCD Message 1 broadcasts.
	Alarm Message Categories	Message Categories 1-8 determine which Area Zone state messages will be displayed on this LCD terminal. Messages will be displayed for Zones that have a matching category set in their Process Group.
Logged Off Keys	Up/Down Arrow Mode None Array Text	Select the Up/Down Arrow key operation for Area Status. No Area status available via the Up/Down Arrow keys. Up/Down Arrow keys will display Area status as an array of 8 Areas per screen. Up/Down Arrow keys will display Area status as a text message, one Area at a time.
	Logged Off Operations. Allow Quick Alarm Review Allow Named Actions Allow Aircon Control Allow Show Info Allow Logged Off Panic	Select the LCD Terminal operations allowed when logged off. Quick Alarm Review allowed via <MENU>, <1>. Named Actions allowed via the > key. Note that the named action must have the “Allow Logged Off Access” option enabled. Aircon Control (Not yet implemented) System Information allowed via <MENU>, <2> . The LCD Terminal “Panic” System Input can be triggered by pressing the <HELP> key 3 times in succession. Note that since this is a “logged off” operation, the LCD Terminal rather than the User will be identified in Review and Reporting messages.
Access Control	Associated Door	Select a Door to be associated to this LCD terminal. The Door nominated will be controlled and monitored by this terminal.
	Access Control Options. Access Only. No Lock. Tongue Sense. Zone 2 Rex Zone 2 Opposite Side	This Terminal may only be used for access control. CAUTION: Once set, you will not be able to access other operations or Menus from this Terminal. Set to ‘Y’ if there is no lock hardware for this Door Allow Tongue Sense logic for this Door. LCD Terminal Zone 2 functions as the Exit (REX) button LCD Terminal Zone 2 REX/REN button is on the Opposite side of the Door to where this Terminal is installed.

	Reader 01 Purpose Control a Door Control a Lift Log On Area Toggle	Reader Purpose defines how the Reader will be used. Door access control. Lift access control. Terminal Logon. A Valid Card presentation logs the User on to the associated LCD Terminal. Area On/Off only. No access control operations.
	Reader 01 Location None Inside Door 1 Outside Door 1	Determines the location of the Terminal in relation to the associated Door; Inside or Outside.
	Keypad Area.	Reader Keypad Area. Select the Area to control when the Reader purpose is “Area Toggle”.
	Reader Type None Magnetic Wiegand	Defines the Data output type for the Reader; Wiegand (D0 / D1) or Magnetic Stripe (Data & Clock).
	Magnetic Card Type Normal (Swipe) Insertion Swipe Last	If “Magnetic” was selected above, this screen will be displayed to select the Magnetic Card Data format to be processed. Normal Card Swipe Reader. Insertion. The data is read in reverse. This option caters for Insertion Card Readers that read the data as the Card is extracted from the Reader. Last. The last, rather than the first characters in the data string are processed. This option is used where the unique card number is in the last part of the card data.
	Wiegand Card Type. N Bit 26 Bit etc.	If “Wiegand” was selected above, this screen will be displayed to define the number of bits to be processed for Wiegand Card types. <i>See 2 Door Reader Module programming for format details.</i>
	Card Format. Direct Entry Wiegand 26Bit Wiegand (H10301) Indala 27 Bit - Wiegand etc.	This screen allows the Card Format to be selected for Magnetic Cards and non-standard Wiegand cards. <i>See 2 Door Reader Module programming for card format details.</i>
	Any Card Mode.	If enabled, any card of the correct type will be allowed access and the card data will be logged to Review.
	PIN Device (Entity for PIN Code Entry)	Select a Module/Reader to be used for entering the PIN Code when Card + PIN is required.

	Wiegand PIN Mode. None Motorola HID Reader MR Access Model Reader 26 Bit Wiegand Keypad IR Weatherproof Terminal 26 Bit Wiegand Keypad Forced	Select the PIN data mode if a Reader” was selected in the “PIN Device” option above. No PIN entry requirement. Motorola/Indala ARK-501 HID 5355 or iClass with 4 Bit Burst PIN output format. MR Access Magnetic Swipe & PIN code Reader 26 Bit Wiegand Keypad. Inner Range Weatherproof Terminal. 26 Bit Wiegand Keypad Forced.
	Reader Arming Mode No Reader Arming User Area w/button Area Empty Exit Area w/button Entry Area w/button Exit Area on 3 Swipes Entry Area on 3 Swipes	Select the Area Arming Mode if the Reader is to be used for Area Arming on Access Control operations. No Arming. Arm the User Area if the “Arm” button is pressed while the Card is presented. Arm the Exit Area (Area you are leaving) if the Area User Count decrements to zero when the Card is presented. Arm the Exit Area if the “Arm” button is pressed while the Card is presented. Arm the Entry Area if the “Arm” button is pressed while the Card is presented. Arm the Exit Area if Card presented 3 times within 5 seconds. Arm the Entry Area if Card presented 3 times within 5 seconds. NOTE: SOME OF THESE OPTIONS NOT RELEVANT TO LCD TERMINAL. E.g. ARM BUTTON OPERATION. NOTE: The Exit Area is the Area you are leaving. i.e. The Area the Reader is installed in. The Entry Area is the Area on the opposite side of the Door to where the Reader is installed.
Security (Incorrect PIN Lockout)	Lockout attempts	The number of incorrect PIN entries before the LCD terminal is Locked Out. The number of tries must occur within the Attempts Time.
	Keypad Lockout Time	Defines how long this LCD terminal will reject PIN operations once the number of Lockout Attempts has been reached within the Attempts Time.
	Keypad Lockout Attempts timer	PIN attempts Timer. The amount of time in which the Lockout Attempts must be reached before the LCD terminal becomes Locked Out. This is the time required to elapse before the lockout count is reset after an illegal PIN has been entered.
LAN Module settings	Poll Time	Enter a Poll Time in Minutes, Seconds. The Poll time is the maximum amount of time a module can remain out of communication with the Control Module.
	Battery Test Time	Not applicable to Concept LCD Terminals.
	Unibus Modules	Not applicable to Concept LCD Terminals.

	Enable on LAN Disable on LAN	This operation is available by Right-clicking on the Module in the “Navigation” Pane. Provides a facility to temporarily disable a faulty Module on the LAN and Isolate its Inputs while awaiting service.
Extra Restrictions.	What When	Up to 6 Permissions can be assigned to an LCD Terminal to place additional restrictions on the operations allowed to be performed. e.g. A limited permission set may be required at particular LCD Terminals during certain times of the day, or while a particular Area is armed or disarmed. Defines the entity for this Permission. e.g. Menu Group, Area List, etc. Defines when the entity is valid for this Permission. e.g. Time Period, Area state, etc. <i>See Permission programming in “Generic Programming Operations” for details.</i>

Expander

Entity/Feature	Option	Description
Find Expander		Select Record to Alter.
Module Name		Program a name of up to 32 characters in length. Use this feature to describe the location and/or purpose of the Module.
Inputs	EOL (End-Of-Line) Scheme	Select the End Of Line Resistor scheme to be used for the Zone Inputs. An EOL scheme can be selected for each block of 8 Zone Inputs: Block 1: Zones 1 to 8 Block 2: Zones 9 to 16 Block 3: Zones 17 to 24 Block 4: Zones 25 to 32
Analogue hysteresis		Enter an Analogue Hysteresis value. This is the sensitivity to changes in analogue values to initiate a change of state. NOTE: Used for legacy Concept 3000 Analogue Modules only. For Integriti Expanders, this option is set in the relevant Input programming.
LAN Module settings	Poll Time	Enter a Poll Time in Minutes, Seconds. The Poll time is the maximum amount of time a module can remain out of communication with the Control Module.
	Battery Test Time	Enter a Battery Test Time in Hours and Minutes. Determines the battery test time for this Module.
	Unibus Modules	Define the Unibus Modules installed on relevant types of Integriti Expander Modules. Not relevant for Concept Expanders.

	Enable on LAN Disable on LAN	This operation is available by Right-clicking on the Module in the “Navigation” Pane. Provides a facility to temporarily disable a faulty Module on the LAN and Isolate its Inputs while awaiting service.
AC Holdoff Time		Specifies the period that an AC Fail condition may exist before the AC Fail System Input is triggered for this Module.

2-Door Reader Module

Entity/Feature	Option	Description
Find 2-Door Reader Module		Select Record to Alter.
Module Name		Program a name of up to 32 characters in length. Use this feature to describe the location and/or purpose of the Module.
Readers. These options are programmed separately for Reader 1 and Reader 2.	Reader Purpose Control a Door Control a Lift Log On Area Toggle	Reader Purpose defines how the Reader will be used. Door access control Lift access control Terminal Logon. A Valid Card presentation logs the User on to the associated LCD Terminal. Area On/Off only. No access control operations.
	Reader Location None Inside Door 1 Outside Door 1 Inside Door 2 Outside Door 2	Determines which Door the Reader is associated with, and the location of the Reader in relation to the Door; Inside or Outside. Reader is not associated with a Door. Reader is located Inside the 1 st Door. Reader is located Outside the 1 st Door. Reader is located Inside the 2nd Door. Reader is located Outside the 2nd Door.
	Keypad Area.	Reader Keypad Area. Select the Area to control when the Reader purpose is “Area Toggle”.
	Reader Type None Magnetic Wiegand	Defines the Data output type for the Reader; Wiegand (D0 / D1) or Magnetic Stripe (Data & Clock).
	Magnetic Card Type Normal (Swipe) Insertion Swipe Last	If “Magnetic” was selected above, this screen will be displayed to select the Magnetic Card Data format to be processed. Normal Card Swipe Reader. Insertion. The data is read in reverse. This option caters for Insertion Card Readers that read the data as the Card is extracted from the Reader. Last. The last, rather than the first characters in the data string are processed. This option is used where the unique card number is in the last part of the card data.

	Wiegand Card Type. N Bit 26 Bit 27 Bit 30 Bit 32 Bit 34 Bit 35 Bit 36 Bit 37 Bit Secure 40	If “Wiegand” was selected above, this screen will be displayed to define the number of bits to be processed for Wiegand Card types. Wiegand Card data of any length up to 88 bits. 26 Bits 27 Bits 30 Bits 32 Bits 34 Bits 35 Bits 36 Bits 37 Bits Inner Range Secure 40 Card data.
	Card Format. Direct Entry Wiegand 26Bit Wiegand (H10301) Indala 27 Bit - Wiegand Keri 30 Bit Wiegand Ind/Kant KSF 32Bit W... HID 32 Bit Wiegand KASTLE 32Bit Wiegand HID 34Bit Wiegand (H1... Indala 34Bit Wiegand HIDCorp1000 35Bit (H5... HID 35 Bit Wiegand Indala 36 Bit Wiegand HID 36Bit Wieg (Std) HID 36Bit Wiegand (S9... HID 37Bit No SC (H10302) HID 37Bit SC (H10304) HID iClass 37Bit Wiegand BQT 38Bit Wiegand HID 40Bit Wiegand IR Secure40 Wiegand IRMag Secure C3K Mag Direct Integriti Mag Direct	This screen allows the Card Format to be selected for Magnetic Cards and non-standard Wiegand cards. If the required format is not in the list, additional Card Formats can be added via Card Format programming. Direct Entry Wiegand HID 26 Bit Wiegand (H10301) Indala 27 Bit Wiegand Keri 30 Bit Wiegand Indala / Kantech KSF 32 Bit Wiegand HID 32 Bit Wiegand KASTLE Wiegand Swipe Card 32 Bit HID 34 Bit Wiegand (H10306) Indala 34 Bit Wiegand HID Corporate 1000 35 Bit Wiegand (H50360) HID 35 Bit Wiegand Indala 36 Bit Wiegand HID 36 Bit Wiegand (Std) HID 36Bit Wiegand (S906133A) HID 37 Bit Wiegand with No Site Code (H10302) HID 37 Bit Wiegand with Site Code (H10304) HID iClass 37 Bit Wiegand BQT 38 Bit Wiegand HID 40 Bit Wiegand Inner Range Secure40 Inner Range Magnetic Card Secure Site Code Concept 3000/4000 Magnetic Card Direct Entry Integriti Magnetic Card Direct Entry
	Any Card Mode.	Any card of the correct type will be allowed access and the card data will be logged to Review.
	PIN Device (Entity for PIN Code Entry)	Select a Module/Reader to be used for entering the PIN Code when Card + PIN is required.
	Wiegand PIN Mode. None Motorola HID Reader MR Access Model Reader 26 Bit Wiegand Keypad IR Weatherproof Terminal 26 Bit Wiegand Keypad Forced	Select the PIN data mode if a Reader” was selected in the “PIN Device” option above. No PIN entry requirement. Motorola/Indala ARK-501 HID 5355 or iClass with 4 Bit Burst PIN output format. MR Access Magnetic Swipe & PIN code Reader 26 Bit Wiegand Keypad. Inner Range Weatherproof Terminal. 26 Bit Wiegand Keypad Forced.

	Reader Arming Mode No Reader Arming User Area w/button Area Empty Exit Area w/button Entry Area w/button Exit Area on 3 Swipes Entry Area on 3 Swipes	Select the Area Arming Mode if the Reader is to be used for Area Arming on Access Control operations. No Arming. Arm the User Area if the “Arm” button is pressed while the Card is presented. Arm the Exit Area (Area you are leaving) if the Area User Count decrements to zero when the Card is presented. Arm the Exit Area if the “Arm” button is pressed while the Card is presented. Arm the Entry Area if the “Arm” button is pressed while the Card is presented. Arm the Exit Area if Card presented 3 times within 5 seconds. Arm the Entry Area if Card presented 3 times within 5 seconds. NOTE: The Exit Area is the Area you are leaving. i.e. The Area the Reader is installed in. The Entry Area is the Area on the opposite side of the Door to where the Reader is installed.
Door Access Control	Door 1 (First Associated Door)	Select the first Door to be assigned to this Reader Module. The Door nominated will be controlled and monitored by this Module.
	Settings for first Door. No Lock. Tongue Sense.	No Lock. Set to ‘Y’ if there is no lock hardware for this Door Tongue Sense. Allow Tongue Sense logic for this Door. The state of the Tongue Sense Input will be utilized in functions such as Forced Door, DOTL, Interlocking, etc.
	Door 2 (Second Associated Door)	Select the second Door to be assigned to this Reader Module if required. If this Reader Module is providing Entry and Exit Readers for the same Door, then a second Door is not assigned. The Door nominated will be controlled and monitored by this Module.
	Settings for second Door. No Lock. Tongue Sense.	No Lock. Set to ‘Y’ if there is no lock hardware for this Door Tongue Sense. Allow Tongue Sense logic for this Door. The state of the Tongue Sense Input will be utilized in functions such as Forced Door, DOTL, Interlocking, etc.
	General Door options. No LEDs DOTL Warning	Disable LED Outputs. LEDs will not provide Valid/Invalid indication and will only be controlled by the associated Auxiliary. The local “Door Held Open” warning output will operate on this Module.

Standalone Operation (Offline Options)	Door 1 Entry dual user Door 2 Entry dual user Door 1 Exit dual user Door 2 Exit dual user Door 1 Entry ren button Door 2 Entry ren button Door 1 Exit rex button Door 2 Exit rex button	Standalone Operation options for the Doors assigned to the Module. These requirements will only be relevant while the Module is Offline. Dual User requirement for Entry at first Door. Dual User requirement for Entry at second Door. Dual User requirement for Exit at first Door. Dual User requirement for Exit at second Door. REN button will operate at first Door. REN button will operate at second Door. REX button will operate at first Door. REX button will operate at second Door.
Access Control	Lift Car 1 (First Associated Lift)	Select the first Lift to be assigned to this Reader Module. Access control for the nominated Lift will be provided by this Module.
	Lift Car 2 (Second Associated Lift)	Select the second Lift to be assigned to this Reader Module. Access control for the nominated Lift will be provided by this Module. Note that Reader Modules for Lift Control are often installed in the Lift Car. This means that a second Lift Car is usually not assigned to a Reader Module.
Offline Options.	Card Cache Time None 1 Hour 4 Hours 8 Hours 1 Day 2 Days 4 Days 1 Week 2 Weeks 1 Month 2 Months 4 Months	Select the period for which a Cached Card will be retained in the Cache from the last time it was used.
	Button Cache Time None 1 Hour 4 Hours 8 Hours 1 Day 2 Days 4 Days 1 Week 2 Weeks 1 Month 2 Months 4 Months	Select the period for which a Cached Button operation will be retained in the Cache from the last time it was used.

	Offline Function. None First 2 Credentials Pass Use Cached Credentials	Determines which card credentials the reader will process in offline mode. No Card access when Module is offline. Allow access for the first 2 Backup Cards only when Module is offline. Allow access to Cards stored in the local Cache when Module is offline.
	Button options. REN button works when offline REX button works when offline	REN (Request to Enter) button enabled when Module offline. REX (Request to Exit) button enabled when Module offline.
Inputs	EOL (End of Line) for Zones.	Select the End of Line Resistor Scheme for an Integriti 2-Door Reader Module. Not relevant for Concept 2-Door Reader Modules.
LAN Module	Poll Time	Enter a Poll Time in Minutes, Seconds. The Poll time is the maximum amount of time a module can remain out of communication with the Control Module
	Battery Test Time	Enter a Battery Test Time in Hours and Minutes. Determines the battery test time for this Module.
	Unibus Modules	Define the Unibus Modules installed on Integriti Reader Modules. Not relevant for Concept 2-Door Reader Modules.
	Enable on LAN Disable on LAN	This operation is available by Right-clicking on the Module in the “Navigation” Pane. Provides a facility to temporarily disable a faulty Module on the LAN and Isolate its Inputs while awaiting service.

Integriti Graphic Terminal

Entity/Feature	Option	Description
Find Graphic Terminal		Select Record to Alter.
Module Name		Program a name of up to 32 characters in length. Use this feature to describe the location and/or purpose of the Module.
General Options	Associated Area	Determines the Associated Area for this Terminal. Used in conjunction with other Terminal options.
	Graphic Terminal Options No Keypad Beep. Entry Display. Entry Beep. Exit Display. Exit Beep.	Select the general Terminal options required. No feedback beep when keys are pressed. Show Entry Timer countdown for the associated Area. Beep during entry timer for the associated Area. Show Exit Timer countdown for the associated Area. Beep during exit timer for the associated Area.

	LED Mode. None Area Array (Red / Off) Area Array (Red / Green) Auxiliary Idle Entities	Select the default LED operation for the eight LEDs across the top of the Graphic Terminal. For the purposes of this option, the LEDs are numbered 1 to 8 from Left to Right. No LED control. LEDs will display Area status by default with Red LEDs only. (Red = Armed) LEDs will display Area status by default with Red and Green LEDs. (Red = Armed) LEDs are controlled by their associated Auxiliary only. Graphic Terminal Auxiliaries 9 to 16 are used for this purpose. i.e. LED 1=Gnn:X09, LED 2=Gnn:X10, etc. When the Terminal is logged off, the LEDs will display the current state of up to eight entities selected in the “Idle Entities” option described below. If more than eight Entities are selected, the LEDs will display the status of the first eight.
	EOL Index	Select the End Of Line Resistor scheme to be used for the Zone Inputs.
Logged Off Display	Idle Entities.	Up to 10 entities may be chosen for which the Graphic Terminal will display the current state. Currently, Areas are the only Entity relevant to this option. Via the Screen: The state of the selected Entities will be displayed in the selected circumstances on the Colour Graphic Screen when the Terminal is logged off and the “Idle Entities” setting is chosen in one or more of the Logged Off Display options. Via the LEDs: The state of up to 8 of the selected Entities will be displayed on the LEDs when the Terminal is logged off and the “Idle Entities” setting is chosen in the “LED Mode” option.
	Idle Display. System Ready System Time Single Area Idle Entities Time Digital Time Analogue Zones Icons	This message will be displayed on the Graphic Terminal Colour display whilst logged off. The text “System Ready” is displayed The current system time and date is displayed. The status of the Associated Area is displayed The Icons, Names and Status of the selected “Idle Entities” is displayed. Time is displayed in digital format. Time is displayed in analogue (clock face) format. Not currently supported. Four logged off menu icons are displayed. (PIN Code, Review, Information and Control)
	Idle Area Off Display.	This alternative message will be displayed on the Graphic Terminal if an associated Area has been assigned to the Terminal, and that Area is Off. Options as above.

	Display options Display Alarm Messages. Display Status Messages. Display LCD Messages. Display Input Levels. Display Area Arm Warning.	Select the types of messages that the Terminal is allowed to accept. Area Alarm Messages allowed. Area Alarm Message Categories must also be programmed. Select whether terminal will display System Status messages such as Power Supply, Battery, Communication or LAN Network problems. Select whether terminal will display custom LCD Messages. An LCD Message, if Valid, will override the selected Idle Display. Input Level messages allowed. (Limited Messages) Restricts the LCD Messages to the Defer Arm Warning (“Area about to turn on”) and LCD Message 1 broadcasts.
	Alarm Message Categories	Message Categories 1-8 determine which Area Zone state messages will be displayed on this Terminal. Messages will be displayed for Zones that have a matching category set in their Process Group.
	Logged Off Operations. Allow Quick Alarm Review Allow Named Actions Allow Aircon Control Allow Show Info Allow Logged Off Panic	Select the Terminal operations allowed when logged off. Quick Alarm Review allowed via <MENU>, <2>. Named Actions allowed via <MENU>, <1>. Note that the named action must have the “Allow Logged Off Access” option enabled. Aircon Control allowed via <MENU>, <3>. (Not yet implemented) System Information allowed via <MENU>, <4>. The Terminal “Panic” System Input can be triggered by pressing the <HELP> key 3 times in succession. Note that since this is a “logged off” operation, the Terminal rather than the User will be identified in Review and Reporting messages.
Access Control	Associated Door	Select a Door to be associated to this Terminal. The Door nominated will be controlled and monitored by this terminal.
	Access Control Options. Access Only. No Lock. Tongue Sense.	This Terminal may only be used for access control. CAUTION: Once set, you will not be able to access other operations or Menus from this Terminal. Set to ‘Y’ if there is no lock hardware for this Door Allow Tongue Sense logic for this Door.
	Dual Code Wait Time.	Enter a Dual Code Time in Minutes and Seconds. Determines how long this Terminal will wait for the second PIN Code in a dual PIN entry.
	Reader 01 Purpose Control a Door Control a Lift Log On Area Toggle	Reader Purpose defines how the Reader will be used. Door access control. Lift access control. Terminal Logon. A Valid Card presentation logs the User on to the associated LCD Terminal. Area On/Off only. No access control operations.

	Reader 01 Location None Inside Door 1 Outside Door 1	Determines the location of the Terminal in relation to the associated Door; Inside or Outside.
	Keypad Area.	Reader Keypad Area. Select the Area to control when the Reader purpose is “Area Toggle”.
	Reader Type None Magnetic Wiegand	Defines the Data output type for the Reader; Wiegand (D0 / D1) or Magnetic Stripe (Data & Clock).
	Magnetic Card Type Normal (Swipe) Insertion Swipe Last	If “Magnetic” was selected above, this screen will be displayed to select the Magnetic Card Data format to be processed. Normal Card Swipe Reader. Insertion. The data is read in reverse. This option caters for Insertion Card Readers that read the data as the Card is extracted from the Reader. Last. The last, rather than the first characters in the data string are processed. This option is used where the unique card number is in the last part of the card data.
	Wiegand Card Type. N Bit 26 Bit etc.	If “Wiegand” was selected above, this screen will be displayed to define the number of bits to be processed for Wiegand Card types. <i>See 2 Door Reader Module programming for format details.</i>
	Card Format. Direct Entry Wiegand 26Bit Wiegand (H10301) Indala 27 Bit - Wiegand etc.	This screen allows the Card Format to be selected for Magnetic Cards and non-standard Wiegand cards. <i>See 2 Door Reader Module programming for card format details.</i>
	Any Card Mode.	If enabled, any card of the correct type will be allowed access and the card data will be logged to Review.
	PIN Device (Entity for PIN Code Entry)	Select a Module/Reader to be used for entering the PIN Code when Card + PIN is required.
	Wiegand PIN Mode. None Motorola HID Reader MR Access Model Reader 26 Bit Wiegand Keypad IR Weatherproof Terminal 26 Bit Wiegand Keypad Forced	Select the PIN data mode if a Reader” was selected in the “PIN Device” option above. No PIN entry requirement. Motorola/Indala ARK-501 HID 5355 or iClass with 4 Bit Burst PIN output format. MR Access Magnetic Swipe & PIN code Reader 26 Bit Wiegand Keypad. Inner Range Weatherproof Terminal. 26 Bit Wiegand Keypad Forced.

	Reader Arming Mode No Reader Arming User Area w/button Area Empty Exit Area w/button Entry Area w/button Exit Area on 3 Swipes Entry Area on 3 Swipes	Select the Area Arming Mode if the Reader is to be used for Area Arming on Access Control operations. No Arming. Arm the User Area if the “Arm” button is pressed while the Card is presented. Arm the Exit Area (Area you are leaving) if the Area User Count decrements to zero when the Card is presented. Arm the Exit Area if the “Arm” button is pressed while the Card is presented. Arm the Entry Area if the “Arm” button is pressed while the Card is presented. Arm the Exit Area if Card presented 3 times within 5 seconds. Arm the Entry Area if Card presented 3 times within 5 seconds. SOME OF THESE OPTIONS NOT RELEVANT TO GRAPHIC TERMINAL. I.E. ARM BUTTON OPERATION? NOTE: The Exit Area is the Area you are leaving. i.e. The Area the Reader is installed in. The Entry Area is the Area on the opposite side of the Door to where the Reader is installed.
Security (Incorrect PIN Lockout)	Lockout attempts	The number of incorrect PIN entries before the Terminal is Locked Out. The number of tries must occur within the Attempts Time.
	Keypad Lockout Time	Defines how long this Terminal will reject PIN operations once the number of Lockout Attempts has been reached within the Attempts Time.
	Keypad Lockout Attempts timer	PIN attempts Timer. The amount of time in which the Lockout Attempts must be reached before the Terminal becomes Locked Out. This is the time required to elapse before the lockout count is reset after an illegal PIN has been entered.
LAN Module settings	Poll Time	Enter a Poll Time in Minutes, Seconds. The Poll time is the maximum amount of time a module can remain out of communication with the Control Module.
	Battery Test Time	Not applicable to Graphic Terminals.
	Unibus Modules	Not currently applicable to Graphic Terminals.
	Enable on LAN Disable on LAN	This operation is available by Right-clicking on the Module in the “Navigation” Pane. Provides a facility to temporarily disable a faulty Module on the LAN and Isolate its Inputs while awaiting service.

Extra Restrictions.	What When	Up to 6 Permissions can be assigned to a Graphic Terminal to place additional restrictions on the operations allowed to be performed. e.g. A limited permission set may be required at particular Terminals during certain times of the day, or while a particular Area is armed or disarmed. Defines the entity for this Permission. e.g. Menu Group, Area List, etc. Defines when the entity is valid for this Permission. e.g. Time Period, Area state, etc. <i>See Permission programming in “Generic Programming Operations” for details.</i>
Associated Air-conditioning unit		Not yet implemented.

RF Expander

Entity/Feature	Option	Description
Find RF Module		Select Record to Alter.
Name		Program a name of up to 32 characters in length. Use this feature to describe the location and/or purpose of the Module.
Inputs	EOL	Not relevant to RF Expanders.
Sensor Registry.	RF Sensor ID 1 to 32 (HEX)	View or Enter the RF device IDs for registration with this module. The device ID is entered in HEXADECIMAL format. Up to 32 devices can be registered with an RF Expander Module.
LAN Module	Poll Time	Enter a Poll Time in Minutes and Seconds. The Poll time is the maximum amount of time a module can remain out of communication with the Control Module.
	Battery Test Time	Not relevant to the current range of RF Expander Modules.
	Unibus Modules	Not relevant to the current range of RF Expander Modules.
	Enable on LAN Disable on LAN	This operation is available by Right-clicking on the Module in the “Navigation” Pane. Provides a facility to temporarily disable a faulty Module on the LAN and Isolate its Inputs while awaiting service.
Miscellaneous RF Expander Options	OK Feedback Action None Control Area Control Area List Control Aux Control Aux List Etc.	Allows an entity to be chosen to provide feedback for “OK” indication. e.g. A Siren Chirp, or an Auxiliary that controls a Beeper. When an action entity is selected additional options will be displayed to program the remaining action settings. <i>See Action programming in “General Programming Operations for programming details.</i>

	RF Poll Time.	Enter a Transmitter Poll Time in Hours. The Poll time is the maximum amount of time an RF device can remain out of communication with the RF Expander Module.
	General RF Expander Options US Jamming Log Missed RF. Log RF Zone Details. Log RF Remote Details.	Enable US Jamming detection algorithm. An event is logged to Review to indicate re-synchronizing of a Fob that is slightly out of sync with the Receiver. Logs Wireless Sensor activity to Review. Logs Wireless Remote activity to Review.

LAN Power Supply Module

Calibration

LAN Power Supply Modules are calibrated at the factory during the manufacturing process. The Module does not normally require any further calibration unless the Module's firmware is upgraded, or a repair has been carried out that required components to be replaced.

Any Firmware upgrade or repair work performed by the manufacturer will also include re-calibration of the Module.

In the rare event of a firmware upgrade being performed in the field, a calibration procedure is available from the Distributor. The following equipment is required to perform the calibration procedure:

- A Digital Multimeter capable of measuring 0 to 20V DC and 0 to 1999mA DC.
- Dummy load. 10 to 15 Ohms. 15W. e.g. 12V, 15Watt Automotive lamp.
- Heavy guage (14/020) test leads for connection of Dummy load and Multimeter.

Entity/Feature	Option	Description
Find LAN Power Supply Module		Select Record to Alter.
LAN Power Supply Name		Program a name of up to 32 characters in length. Use this feature to describe the location and/or purpose of the Module.
LAN Power Supply Options	Invert Auxiliary 1 Invert Auxiliary 2.	Invert the operation of Auxiliary 1. Invert the operation of Auxiliary 2. Normally set to "Y" when a Satellite Siren is connected to this output. <i>See Note below.</i> IMPORTANT NOTE: Auxiliary 2 is <u>not</u> an Open Collector output. It provides a switched +12V output via an on-board relay and can therefore be used to control a Battery-backed Satellite Siren or other similar controlled device. - When used for controlling a Battery-backed Satellite Siren, the 12V output normally needs to be <u>present</u> when the Auxiliary is <u>Off</u> , and <u>removed</u> when the Auxiliary is <u>On</u> . Therefore, the "2" option must be set to "Y". - When controlling a device such as a Strobe or Piezo Siren (where the 12V output needs to be present when the Auxiliary is ON) the "2" option must be set to "n".
LAN Module	Poll Time	Enter a Poll Time in Minutes and Seconds. The Poll time is the maximum amount of time a module can remain out of communication with the Control Module.
	Battery Test Time	Enter a Battery Test Time in Hours and Minutes. Determines the battery test time for this Module.

	Unibus Modules	Define the Unibus Modules installed on relevant types of Integriti Expander Modules. Not relevant for Concept LAN Power Supply Modules.
	Enable on LAN Disable on LAN	This operation is available by Right-clicking on the Module in the “Navigation” Pane. Provides a facility to temporarily disable a faulty Module on the LAN and Isolate its Inputs while awaiting service.
Miscellaneous LAN Power Supply Options.	Number of Slaves	Specifies the number of Slave Modules connected to a Master LAN Power Supply Module. Up to 3 Slave Modules can be connected. The default setting of 0 indicates that no Slave Modules are connected and disables the Slave Fail System Input for this LAN Power Supply Module. Slave Modules are connected to provide additional Battery charging current AND/OR Detector current on a LAN Power Supply Module. This is done by connecting additional “Slave” LAN Power Supply Modules to the 2-wire Slave Bus connection provided, and connecting the “+B” and “DET+” outputs of the Slave Module to the “+B” AND/OR “DET+” output of the Master Module. IMPORTANT NOTE: <i>See the Installation Manual for DIPswitch settings, wiring information and additional details.</i>
	Batt Overcurrent Detector Overcurrent	These options allow the Installer to independently specify the maximum current allowed from the Battery Charger circuit and the Detector Supply circuit before Over-current System Input Alarms are activated. The value is programmed in milliAmps, and can be set from 0.1A (100mA) to 9.9 Amps in 100mA increments. A value of 00 means that the Over-current condition is not monitored. <i>See Important Notes below.</i>

	IMPORTANT NOTES: 1. 2. 3. CALCULATING THE MAXIMUM CURRENT AVAILABLE. <u>Example 1:</u> <u>Example 2:</u>	- If using the Standard version of the Module, or an Enhanced version with <u>no</u> Slave Modules connected, the value should be set to no more than 4A. - If the Enhanced version is used, <u>and</u> Slave Modules are connected, a value of up to 9.9A may be set depending on the number of Slave Modules connected and the wiring configuration. - If the Master/Slave configuration chosen is designed to deliver more than 9.9A on a particular circuit, then Over-current monitoring for that circuit must be disabled. (Set value to 00) <i>See examples below.</i> The Maximum Battery Current or Detector Current available is calculated as follows: $I_{max} = 2 + 2n$ Where “n” is the number of Slave Supply outputs (“+B” and/or “DET+” outputs) connected to the specified Master output. If one Slave is connected, set to “Charger Only Mode” and +B / -B of the Slave is connected to +B / -B on the Master, then the maximum <u>Battery</u> current available would be $2 + (2 \times 2) = 6A$. “Charger Only Mode” combines the current available from the 2 outputs into the specified output. (In this case, the maximum guaranteed Detector current available would remain at 2A) If three Slaves are connected, set to “Split Mode” and: - +B / -B from all Slaves is connected to +B / -B on the Master. - DET+ / 0V from all Slaves is connected to DET+ / 0V on the Master. Then; The maximum <u>Battery</u> current available would be $2 + (2 \times 3) = 8A$; And the maximum <u>Detector</u> current available would also be $2 + (2 \times 3) = 8A$.
	Aux 2 Undercurrent	Specifies the minimum current required to prevent a Satellite Siren Tamper Alarm condition. The value should be set from 20 to 50mA in 1mA increments. The default value of 00 means that Aux2 Tamper current is not monitored. NOTE: Any value less than “20” disables Aux2 Tamper current monitoring.

Integriti Four Door Access Module (Not yet available)

Entity/Feature	Option	Description
Find 4-Door Access Module		

Concept Analogue Module (Not yet supported)

Entity/Feature	Option	Description
Find Analogue Module		

Controller – Module Details

Entity/Feature	Option	Description
Module Name		Program a name of up to 32 characters in length. Use this feature to describe the location and/or purpose of the Module.
Inputs	EOL (End-Of-Line) Scheme Concept 3K 8-State	Select the End Of Line Resistor scheme to be used for the Zone Inputs. An EOL scheme can be selected for each block of 8 Zone Inputs: Block 1: Zones 1 to 8 Block 2: Zones 9 to 16 Block 3: Zones 17 to 24 Block 4: Zones 25 to 32
Locale Settings	Country None Australia New Zealand Great Britain Czech Republic Poland Netherlands Sweden Hungary Iceland Ireland Norway	Select the Country in which the Controller is being installed. This ensures that Controllers comply with local standards. e.g. Operation of the built-in modem complies with local telecommunications standards.
General Behaviour	Salto Cache Duration Override EOL Force Input Review PIN +1 Duress Save Review to USB	The period of time for which the Salto Locks will cache valid cards. Program a value in Days. Force Input Review. Overrides any Input “No Review” settings forcing all Inputs to log activity to Review. PIN+1 Duress. Enables any security PIN Code to be incremented by 1 to generate a Duress Alarm at a Terminal. e.g. Normal PIN is 1234. Use 1235 for Duress. Normal PIN is 6789. Use 6780 for Duress. USB Review. Save review data to a USB Drive if one is attached.
	AC Holdoff Time	The AC Fail Holdoff time, is the period of time required to pass before the control module registers an AC fail. This allows for brief AC mains supply outages to occur without triggering an AC Fail Alarm. Enter a value in Hours, Minutes and Seconds. A value of up to 18 Hrs, 12 Mins and 15 Seconds can be entered.

	Warning Time.	Global Area Defer Arming warning time for all deferred arming Areas. Determines the Warning Time that will be provided prior to an Area Arming when it has a Defer Arm Timer running. The Warning time starts when the Defer timer expires. Therefore, if no User action is taken, the total time that the Area is Timed Off is the Defer time + the Warning Time. Enter a value in Hours, Minutes and Seconds up to a maximum of 1 Hour, 49 Minutes and 13 Seconds.
	Dual Wait Time.	Determines the length of the wait timer for Dual User and Card & PIN operations. Enter a value in Hours, Minutes and Seconds up to a maximum of 18 Hours, 12 Minutes and 15 Seconds.
	Maximum Review Level	Sets the Maximum Level of Review that will be saved. Selecting the Review Level determines how much detail is provided in the Review Log. Higher Review Levels will log more events to provide additional detail. Lower levels will allow the Review log to cover a longer period of time, but will provide less detail. NOTE: Do not change the default setting unless you understand the ramifications. Lowest Level of detail. Most detailed Level. Recommended, especially during system installation and commissioning.
	Fixed PIN Code length.	Determines a fixed number of PIN digits for User access codes. Enter a number between 1 and 8. A setting of 4 or less is NOT recommended.
Connectivity:	Rings to Answer	Set the number of rings before the Controller's Modem will answer the call.
Connectivity: Serial Reader Settings	Serial Channel None Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) Modem USB Slave USB Master IAC Onboard RS485	IAC ONLY. NOT YET SUPPORTED. No Modem connection. On-board "Port 0" connection. Unibus UART 1, Port 1 Unibus UART 1, Port 2 Unibus UART 2, Port 1 Unibus UART 2, Port 2 Unibus UART 3, Port 1 Unibus UART 3, Port 2 Unibus UART 4, Port 1 Unibus UART 4, Port 2

	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	
	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	
	Stop Bits 1 Bit 2 Bits	
Lockout Settings	User Lockout EN 50131 Operation	Set this option to lockout all Users with the “Lockout Enabled” option set while any Area is Armed. EN50131 Alarm processing. Enable system-wide functionality pertinent to EN50131 (European standards for Intruder Alarm Systems)
Battery Test Settings	Day of Week Sunday Monday Tuesday Wednesday Thursday Friday Saturday	Select the Day of the Week on which the System Battery Test will commence.
	Weeks between Tests	Battery Test frequency. Program the number of Weeks to elapse between each Battery Test. A value between 0 – 255 may be entered. A setting of 0 disables Battery Testing. A setting of 1 to 4 weeks is typical. If the system is being installed to a specific standard, ensure that the Battery Test settings comply with the standard.
	Battery Test Hour	Program the Hour for the Start of the Battery Test. Hours. Enter a value between 0 - 23.
	Battery Test Minute	Program the Minute for the Start of the Battery Test. Minutes. Enter a value between 0 - 59.

Time Report	Hour of the Day	Program the Hour of the Day that the Periodic Test Report will be sent to the Monitoring Station. Note that the Time Report System Input must be assigned to an Area with an appropriate Process Group.
	Day of Week Sunday Monday Tuesday Wednesday Thursday Friday Saturday	Program the Day of the Week that the Periodic Test Report will be sent to the Monitoring Station. One or more days may be selected.
Default Modules	Default RF Reader	Defines the default RF Expander Module that will be used for enrolling Wireless Remotes. e.g. Paradox REM devices or Visonic Remotes.
LAN Module Options	Poll Time	Not Relevant to Control Modules.
	Battery Test Time	Enter a Battery Test Time in Hours and Minutes. Determines the duration of battery test time for the main Control Module C01. (Battery test times for other Modules are set within the options for each individual Module) Enter a value in Days, Hours and Minutes. Battery Test times are determined by the Battery capacity, the normal total load (which includes the Module itself, and its peripherals), and the battery charge required to be retained at the end of the test (to allow for AC failure occurring shortly after the end of a battery test). e.g. For a 7.0 AH battery required to deliver 1.2 Amps during an AC Failure, a battery test time of 3 hours would discharge the battery to just under half its capacity. A Value of up to 45 days, 12 Hours and 15 Minutes may be entered.
	Unibus Modules	Lists the Unibus Modules connected to this Controller.
Basic Details	Controller ID	Records the ID for this Control Module.

Controller – Connection Details

Entity/Feature	Option	Description
Basic Details	Serial Number	Records the Controller Serial Number.
Connectivity	Connection Mode Auto Manual Disabled	

	Preferred Connection Type TCP USB Serial IModem EModem Sky Tunnel Phantom	
	Connection Timeout	Program a connection timeout time in milliseconds. The connection will be closed if the Controller does not send at least one packet within this time. The default setting of 30000 should be retained unless advised otherwise.
	Connection Poll Time	Program a Poll time in milliseconds. This is the maximum amount of time between heartbeat messages and must not exceed the Connection Timeout time above. The default setting of 10000 should be retained unless advised otherwise.
	Modem Serial Port	The Computer Serial Port that a PSTN Modem is connected to when a Modem connection is to be available.
	Modem Configuration String	Optional modem configuration string if a special string is required to configure the modem.
	Modem Phone Number	The telephone number for the PSTN Modem
	Sky Tunnel Pairing Code	The Code used to establish connectivity via Sky Tunnel. This can be found via MENU, 7, 3, 9 at an LCD Terminal.
Synchronisation	Review Synchronisation Mode	Select a Review Synchronisation Mode to determine the point from which Review will be synchronised, and how much Review will be synchronized.
	All Historical Review	Will synchronize Review from the oldest event to the newest event. Note that if the Controller has accumulated a large Review log, this may take some time.
	From Now	Will synchronize Review from the point of time of the connection being established between the Controller and the software.
	Continuous Don't Sync Review	? Review will not be synchronized.
	Don't Sync Time Upon Connection	Option to not synchronise the Controller and Server time upon connection.
	Time Zone	Defines the Time Zone of the location that the Controller is installed in.
	Enable Data Synchronisation	Select to allow data synchronisation between the Controller and the Server.
	Data Sync Mode Merge Changes Disallow Changes from Controller Prefer Controller Changes	Determines how conflicting changes are resolved in an entity has been altered while the Controller is offline.

	Prevent State Syncing	Select to prevent the state of anything connected to the Controller from being synchronised.
Version	Protocol Version	Records the Controller's protocol version
	Firmware Version	Records the version of the Firmware currently installed on the Controller.
Smart Card	Smart Card Serial Number	The Serial Number of the Smart Card installed in the Controller.

Concept Intelligent 4-Door Access Module

V5 or later IFDAM Firmware release introduces support for Integriti Controllers V2.0 or later.

To enable Integriti mode.

Before power-up, set Switch 4 on the Options DIPswitch (S1) to ON.

i.e. S1 Switch 4 OFF = Concept 4000.

S1 Switch 4 ON = Integriti Security Controller.

All other switches on S1 are set to OFF, unless the alternate AC Fail Delay time is required via Switch 2.

This setting causes the IFDAM to act similar to an Integriti 2-Door Reader with an offline cache of 2000 Users.

Note that the mode must be selected to match the type of Control Module that the IFDAM is to be used with.

If the mode does not match the Controller, the IFDAM Fault LEDs will indicate "Module Unknown"

(L2 = OFF, L3 = ON).

Operation in an Integriti System.

GENERAL OPERATION:

- Battery testing is operational.
- The fast unlock time option via Switch 8 on DIPswitch S1 is not supported.

ACCESS CONTROL OPERATIONS WHEN ONLINE:

In online mode, operation should be identical to an Integriti Two-Door Reader or Four-Door Reader Module.

ACCESS CONTROL OPERATIONS WHEN OFFLINE:

In offline mode, the IFDAM can use cached User/Button operations to provide access as follows:

- The cache contains up to 2000 User credentials.
- The cache can be cleared by setting Switch 8 on the Options DIPswitch (S1) to ON (as well as Switch 4) and power cycling the IFDAM. If Switch 8 is left on, then every power cycle will clear the cache.
- When a User is granted access whilst online, the User will be cached for that Door. If the cache is full then the oldest User will be replaced by the new User.
- If a User is denied access, then that User will be removed from the cache for that Door. If they are not in the cache for any other Doors on that Module, then they will be removed from the cache completely on that Module. NOTE. Certain types of "access denied" events will not cause the User to be removed from the cache. E.g. Denied because the Door is interlocked, Denied because Area is On and User does not have permission to turn off that Area, etc.
- When a User is added to the cache, if the User programming has the "permanent cache" option set, then that User cannot be replaced by a newer User. The User will remain in the cache until removed by a power cycle with Switch 8 on, or if denied access at a Door and also not in the cache for any of the other Doors on that Module.

- In addition to Users being removed if a new User is added when the cache is full, Users can also be automatically removed if they have been in the cache for too long. This time is programmable between 1 hour and 4 months. Note that permanent Users are not removed by time.
- The caching of Users can also be disabled completely.

Note that Users are only added when online and access is granted.

Users are only removed from the Module cache:

- When access is denied for all the Doors on that Module on which the User had previously had an access granted event.
- Via time for non-permanent Users.
- Using a Switch 8 power cycle.

If Users are deleted from the Integriti Database whilst online, they are not removed from the cache. If Users are created whilst online they are not automatically added to the cache.

REX and REN button operations are also cached separately, per Door as follows:

- Whenever a REX/REN is allowed whilst online, the REX/REN for that Door is added to the cache.
- Whenever a REX/REN is denied whilst online, the REX/REN for that Door is removed from the cache.
- Cached buttons are also removed by time, programmable from 1 hour to 4 months (separate to User cache time) or can be disabled completely.

Whilst offline, whatever is in the cache determines access permissions.

Whatever REX/REN buttons are in the cache will remain operational until they time out.

Whatever Users are in the cache will remain operational until they timeout, unless they are permanent.

“Dual User” and “Card plus PIN” or “PIN only” is not supported in offline mode.

“PIN only” will not work. If a legal card was presented whilst online, even if a PIN was required but was incorrect, the card will still be added to the cache.

No record of User operations is kept whilst off line.

The Door unlock time is set to 5 seconds when offline.

Checking IFDAM Firmware Version.

The IFDAM Firmware Version can be confirmed via an LCD Terminal as follows:

INTEGRITI:

NOTE: ISC Firmware must be V2.0 or later, and IFDAM Firmware must be V5.0 or later.

- Logon to the LCD Terminal and select Module Info. [MENU, 1, 8]
- Press the Down Arrow key (V) as often as required to locate the IFDAM to view. e.g. C3K-IRdr: 03
- Press the OK key. The display will show the current status of the selected IFDAM. e.g. Present and Secure.
- Press the OK key. The display will now show the current firmware version and build number of the selected IFDAM. e.g. 5.0.0_1

Entity/Feature	Option	Description
Find Intelligent 4-Door Access Module		Select Record to Alter.
Module Name		Program a name of up to 32 characters in length. Use this feature to describe the location and/or purpose of the Module.
End-Of-Line Scheme	Concept3K 8-State	Select the End Of Line Resistor scheme to be used for the Zone Inputs. An EOL scheme can be selected for each block of 8 Zone Inputs: Block 1: Zones 1 to 8 Block 2: Zones 9 to 16 Block 3: Zones 17 to 24 Block 4: Zones 25 to 32
Connectivity: RF Device Serial Settings.	Serial Channel None Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) Modem USB Slave USB Master IAC Onboard RS485	Not relevant to Concept Intelligent Reader Module. No Modem connection. On-board "Port 0" connection. Unibus UART 1, Port 1 Unibus UART 1, Port 2 Unibus UART 2, Port 1 Unibus UART 2, Port 2 Unibus UART 3, Port 1 Unibus UART 3, Port 2 Unibus UART 4, Port 1 Unibus UART 4, Port 2
	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	Not relevant to Concept Intelligent Reader Module.
	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	Not relevant to Concept Intelligent Reader Module.
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	Not relevant to Concept Intelligent Reader Module.

	Stop Bits 1 Bit 2 Bits	Not relevant to Concept Intelligent Reader Module.
Connectivity: Serial Reader Settings	Serial Channel None Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) Modem USB Slave USB Master IAC Onboard RS485	Not relevant to Concept Intelligent Reader Module. No Modem connection. On-board "Port 0" connection. Unibus UART 1, Port 1 Unibus UART 1, Port 2 Unibus UART 2, Port 1 Unibus UART 2, Port 2 Unibus UART 3, Port 1 Unibus UART 3, Port 2 Unibus UART 4, Port 1 Unibus UART 4, Port 2
	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	Not relevant to Concept Intelligent Reader Module.
	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	Not relevant to Concept Intelligent Reader Module.
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	Not relevant to Concept Intelligent Reader Module.
	Stop Bits 1 Bit 2 Bits	Not relevant to Concept Intelligent Reader Module.

Offline Options.	Card Cache Time None 1 Hour 4 Hours 8 Hours 1 Day 2 Days 4 Days 1 Week 2 Weeks 1 Month 2 Months 4 Months	Select the period for which a Cached Card will be retained in the Cache from the last time it was used.
	Button Cache Time None 1 Hour 4 Hours 8 Hours 1 Day 2 Days 4 Days 1 Week 2 Weeks 1 Month 2 Months 4 Months	Select the period for which a Cached Button operation will be retained in the Cache from the last time it was used.
Standalone Operation (Offline Options)	Door 1 Entry dual user Door 2 Entry dual user Door 3... Door 1 Exit dual user Door 2 Exit dual user Door 3... Door 1 Entry ren button Door 2 Entry ren button Door 3... Door 1 Exit rex button Door 2 Exit rex button Door 3...	Standalone Operation options for the Doors assigned to the Module. These requirements will only be relevant while the Module is Offline. The four standalone operation options are programmed separately for each of the eight Doors. Dual User requirement for Entry at first Door. Dual User requirement for Entry at second Door. Dual User Entry options continue for Doors 3 to 8. Dual User requirement for Exit at first Door. Dual User requirement for Exit at second Door. Dual User Exit options continue for Doors 3 to 8. REN button will operate at first Door. REN button will operate at second Door. REN button options continue for Doors 3 to 8. REX button will operate at first Door. REX button will operate at second Door. REX button options continue for Doors 3 to 8.
Access Control: Readers. These options are programmed separately for Readers 1 to 16.	Reader Purpose Control a Door Control a Lift Log On Area Toggle	Reader Purpose defines how the Reader will be used. Door access control Lift access control Terminal Logon. A Valid Card presentation logs the User on to the associated LCD Terminal. Area On/Off only. No access control operations.

	Reader Location None Inside Door 1 Outside Door 1 Inside Door 2 Outside Door 2	Determines which Door the Reader is associated with, and the location of the Reader in relation to the Door; Inside or Outside. Reader is not associated with a Door. Reader is located Inside the 1st Door. Reader is located Outside the 1st Door. Reader is located Inside the 2nd Door. Reader is located Outside the 2nd Door.
	Keypad Area.	Reader Keypad Area. Select the Area to control when the Reader purpose is “Area Toggle”.
	Reader Type None Magnetic Wiegand	Defines the Data output type for the Reader; Wiegand (D0 / D1) or Magnetic Stripe (Data & Clock).
	Magnetic Card Type Normal (Swipe) Insertion Swipe Last	If “Magnetic” was selected above, this screen will be displayed to select the Magnetic Card Data format to be processed. Normal Card Swipe Reader. Insertion. The data is read in reverse. This option caters for Insertion Card Readers that read the data as the Card is extracted from the Reader. Last. The last, rather than the first characters in the data string are processed. This option is used where the unique card number is in the last part of the card data.
	Wiegand Card Type. N Bit 26 Bit 27 Bit 30 Bit 32 Bit 34 Bit 35 Bit 36 Bit 37 Bit Secure 40	If “Wiegand” was selected above, this screen will be displayed to define the number of bits to be processed for Wiegand Card types. Wiegand Card data of any length up to 88 bits. 26 Bits 27 Bits 30 Bits 32 Bits 34 Bits 35 Bits 36 Bits 37 Bits Inner Range Secure 40 Card data.

	Card Format. Direct Entry Wiegand 26Bit Wiegand (H10301) Indala 27 Bit - Wiegand Keri 30 Bit Wiegand Ind/Kant KSF 32Bit W... HID 32 Bit Wiegand KASTLE 32Bit Wiegand HID 34Bit Wiegand (H1... Indala 34Bit Wiegand HIDCorp1000 35Bit (H5... HID 35 Bit Wiegand Indala 36 Bit Wiegand HID 36Bit Wieg (Std) HID 36Bit Wiegand (S9... HID 37Bit No SC (H10302) HID 37Bit SC (H10304) HID iClass 37Bit Wiegand BQT 38Bit Wiegand HID 40Bit Wiegand IR Secure40 Wiegand IRMag Secure C3K Mag Direct Integriti Mag Direct	This screen allows the Card Format to be selected for Magnetic Cards and non-standard Wiegand cards. If the required format is not in the list, additional Card Formats can be added via Card Format programming. Direct Entry Wiegand HID 26 Bit Wiegand (H10301) Indala 27 Bit Wiegand Keri 30 Bit Wiegand Indala / Kantech KSF 32 Bit Wiegand HID 32 Bit Wiegand KASTLE Wiegand Swipe Card 32 Bit HID 34 Bit Wiegand (H10306) Indala 34 Bit Wiegand HID Corporate 1000 35 Bit Wiegand (H50360) HID 35 Bit Wiegand Indala 36 Bit Wiegand HID 36 Bit Wiegand (Std) HID 36Bit Wiegand (S906133A) HID 37 Bit Wiegand with No Site Code (H10302) HID 37 Bit Wiegand with Site Code (H10304) HID iClass 37 Bit Wiegand BQT 38 Bit Wiegand HID 40 Bit Wiegand Inner Range Secure40 Inner Range Magnetic Card Secure Site Code Concept 3000/4000 Magnetic Card Direct Entry Integriti Magnetic Card Direct Entry
	Any Card Mode.	Any card of the correct type will be allowed access and the card data will be logged to Review.
	PIN Device (Entity for PIN Code Entry)	Select a Module/Reader to be used for entering the PIN Code when Card + PIN is required.
	Wiegand PIN Mode. None Motorola HID Reader MR Access Model Reader 26 Bit Wiegand Keypad IR Weatherproof Terminal 26 Bit Wiegand Keypad Forced	Select the PIN data mode if a Reader” was selected in the “PIN Device” option above. No PIN entry requirement. Motorola/Indala ARK-501 HID 5355 or iClass with 4 Bit Burst PIN output format. MR Access Magnetic Swipe & PIN code Reader 26 Bit Wiegand Keypad. Inner Range Weatherproof Terminal. 26 Bit Wiegand Keypad Forced.

	Reader Arming Mode No Reader Arming User Area w/button Area Empty Exit Area w/button Entry Area w/button Exit Area on 3 Swipes Entry Area on 3 Swipes	Select the Area Arming Mode if the Reader is to be used for Area Arming on Access Control operations. No Arming. Arm the User Area if the “Arm” button is pressed while the Card is presented. Arm the Exit Area (Area you are leaving) if the Area User Count decrements to zero when the Card is presented. Arm the Exit Area if the “Arm” button is pressed while the Card is presented. Arm the Entry Area if the “Arm” button is pressed while the Card is presented. Arm the Exit Area if Card presented 3 times within 5 seconds. Arm the Entry Area if Card presented 3 times within 5 seconds. NOTE: The Exit Area is the Area you are leaving. i.e. The Area the Reader is installed in. The Entry Area is the Area on the opposite side of the Door to where the Reader is installed.
Access Control: Doors.	Door 1 to Door 8 assignment. (Associated Doors)	Select the Doors to be assigned to this Reader Module. The Doors nominated will be controlled and monitored by this Module.
Access Control: Lift Cars.	Lift Car 1 to Lift Car 8 assignment. (Associated Lift Cars)	Select the Lifts to be assigned to this Reader Module. Access control for the nominated Lifts will be provided by this Module.
Door Settings	Settings for Doors. Access Only No Lock. Tongue Sense.	The Door settings are programmed separately for each of the eight Doors. No Area Control operations will be allowed. Set to ‘Y’ if there is no lock hardware for this Door Allow Tongue Sense logic for this Door. The state of the Tongue Sense Input will be utilized in functions such as Forced Door, DOTL, Interlocking, etc.

Access Control Hardware Mapping	Door Mapping <u>Device Type:</u> Not Present Onboard Hardware Unibus Reader Unibus Door Salto Aperio Serial Reader <u>DIP Switch Setting</u> <u>Number on Device</u>	Door Mapping is used to map the logical Door number on this Module to the Hardware that is to be used for that Door. There 4 logical Doors on a Concept Intelligent 4-Door Access Module. The Door mapping is programmed by defining the following parameters for each logical Door to be used: - The hardware "Device Type". - The "DIP Switch Setting" on the device (if relevant) - The number of the entity on the device. i.e. Number 1 or 2 if the device supports 2 Readers, or 2 Doors. Not present Onboard Hardware. Unibus Reader (2 Readers). Not relevant to C3K IFDAM. Unibus Door (2 Readers / 2 Doors) Not relevant to C3K IFDAM. Salto RS485. Not relevant to C3K IFDAM. Aperio. Not relevant to C3K IFDAM. Serial Reader. Not relevant to C3K IFDAM. Enter a value between 1 and 8. Not relevant to C3K IFDAM. Enter a value between 1 and 2. Not relevant to C3K IFDAM.
	Reader Mapping <u>Device Type:</u> Not Present Onboard Hardware Unibus Reader Unibus Door Salto Aperio Serial Reader <u>DIP Switch Setting</u> <u>Number on Device</u>	Reader Mapping is used to map the logical Reader number on this Module to a hardware Reader Port. There are 8 logical Readers on a Concept Intelligent 4-Door Access Module. The Reader mapping is programmed by defining the following parameters for each logical Reader to be used: - The hardware "Device Type". - The "DIP Switch Setting" on the device (if relevant) - The number of the entity on the device. i.e. Number 1 or 2 if the device supports 2 Readers, or 2 Doors. Not present Onboard Hardware. Unibus Reader (2 Readers). Not relevant to C3K IFDAM. Unibus Door (2 Readers / 2 Doors) Not relevant to C3K IFDAM. Salto RS485. Not relevant to C3K IFDAM. Aperio. Not relevant to C3K IFDAM. Serial Reader. Not relevant to C3K IFDAM. Enter a value between 1 and 8. Not relevant to C3K IFDAM. Enter a value between 1 and 2. Not relevant to C3K IFDAM.
LAN Module	Poll Time	Enter a Poll Time in Minutes, Seconds. The Poll time is the maximum amount of time a module can remain out of communication with the Control Module
	Battery Test Time	Enter a Battery Test Time in Hours and Minutes. Determines the battery test time for this Module.

	Unibus Modules	Define the Unibus Modules installed on Integriti Reader Modules. Not relevant for Concept Intelligent 4-Door Access Modules.
	Enable on LAN Disable on LAN	This operation is available by Right-clicking on the Module in the “Navigation” Pane. Provides a facility to temporarily disable a faulty Module on the LAN and Isolate its Inputs while awaiting service.
Miscellaneous Intelligent Reader Module Options.	Disabled Auxiliary Control Detail Mode No LEDs Override EOL	Auxiliaries 5 to 8 will follow the Door Lock Auxiliaries for each Door respectively when Door is accessed by a disabled User to trigger an automatic Door opening mechanism. The IFDAM Review Log will include additional detail useful during commissioning and troubleshooting. Disable LED Outputs. LEDs will not provide Valid/Invalid indication and will only be controlled by the associated Auxiliary. Override the EOL requirement for REX and REN button Inputs on all Doors on this Module. i.e. Only a Normally Open switch is required.

Communications Programming

Entity/Feature	Option	Description
Comms Tasks		Program/Edit the Communications Tasks. e.g. Integriti software interface, Alarm reporting, etc.
Telephone Numbers		Program/Edit any Telephone numbers that may be required for Dialler Comms Tasks.
DTMF Remote Control		Not yet implemented.
Network Interface Controllers (NICS)		Program/Edit Network Interfaces.
DNS Servers		Program/Edit DNS Servers.

Comms Tasks

Entity/Feature	Option	Description
Comms Tasks	Comms Task to Program: CT01	Select Communications Task to program. Use <UP>/<DOWN> Arrows to scroll, or use digit keys to enter the number.
Comms Task Setup	Type (format). None Integriti Monitor Dialler GSM Automation EMS Securitel Intercom BMS EN 32 Pin Sky Tunnel E Modem	Select the Communications format for this Comms Task. No Comms Task format selected. Integriti Software communications. Monitor Comms Task. Only use if advised by Tech Support. Digital Dialler Alarm Reporting. E.g. IRfast, Contact ID, SIA, etc. Multipath STU or GSM primary or backup reporting. Control, status monitoring and event logging communication protocol for 3 rd Party Systems. e.g. Home/Building Automation, HVAC, etc. Securitel Serial STU format. While the Securitel network is no longer available, the Securitel Serial format is still utilized as the interface to some 3 rd Party communicators. Serial interface to 3 rd Party Intercom products to facilitate integrated access control functionality. Once the required format is selected, ensure that the Comms Task is currently "Idle".
	Mode Normal Backup	Select whether this Comms Task is a normal Task or a Backup Task. This Comms Task is a Primary reporting Comms Task. This Comms Task is a Backup Comms Task to another Comms Task. e.g. It will only be used if the Primary Reporting Comms Task fails to communicate with the monitoring station.

	Backup Comms Task	Specifies the Comms Task number that will be used as the Backup Comms Task if required. The Backup Task will be triggered after the specified number of Attempts on the Primary Task has failed. When programming the nominated Backup Comms Task, it must be set to “Backup” mode.
--	-------------------	--

<u>INTEGRITI FORMAT</u>		The Integriti Comms Task format allows communications with the Integriti Management Software via one or more prioritised communications paths including Ethernet,
Ethernet Connection	Server IP Address	View or Enter the IP Address of the Integriti Server PC.
	TCP Port	View or Enter the Server TCP Port Number. The default Port number (004711) does not normally need to be changed.
	Server Host Name	Select required DNS Server Name. DNS Servers are programmed separately.
Connectivity Paths	Communications Path. Priority 1 None TCP USB Serial IModem EModem 1 Sky Tunnel Phantom	Select the primary communications path to be used for communications with Integriti Management Software. No Path selected. Ethernet. USB Host Port. RS232 Serial Port. (Not currently supported) Internal Modem. On-board PSTN modem. External Modem 1. PSTN or GPRS Modem on a UniBus UART Port. Factory debugging path only.
	Communications Path. Priority 2	Select a secondary communications path to be used for communications with Integriti Management Software. Options as above.
	Communications Path. Priority 3	Select a 3 rd priority communications path to be used for communications with Integriti Management Software. Options as above.
	Communications Path. Priority 4	Select a 4 th priority communications path to be used for communications with Integriti Management Software. Options as above.
	Communications Path Options. Call. Answer.	Select the connection options for the Communications Paths. These options are programmed separately for each of the four Communications Paths that will be used in the system. The Panel will call the Management Software Server. The Panel will Answer calls from the Management Software Server.
Modem connection: General	Telephone Number.	Enter a Telephone Number for the Controller’s modem to call the Integriti Server back on when the Integriti Server requests a Call-back type connection.

Modem connection: Internal modem Options	First Telephone Number.	
	Telephone Number 1	Select a Telephone Number or Telephone Number List to use as the primary Telephone Number in this Comms Path.
	Qualifier (When)	If required, select a Qualifier to define when this Telephone Number will be valid.
	Invert Qualifier	Select Invert Qualifier to enable the Telephone Number when the Qualifier is invalid.
	Second Telephone Number.	
	Telephone Number 2	Select a Telephone Number or Telephone Number List to use as the secondary Telephone Number in this Comms Path.
	Qualifier (When)	If required, select a Qualifier to define when this Telephone Number will be valid.
	Invert Qualifier	Select Invert Qualifier to enable the Telephone Number when the Qualifier is invalid.
	Maximum Online Time	Determines the maximum time that the Integriti Management Software is allowed to remain connected via this Modem Path. NOT YET IMPLEMENTED.
	Maximum Dial Attempts	Determines the maximum dial attempts this Comms Task will use to contact the Integriti software. When the maximum attempts are reached, the Backup Task, if defined, will be triggered. NOT YET IMPLEMENTED.
Modem connection: External modem Options. NOT YET IMPLEMENTED	First Telephone Number.	
	Telephone Number 1	Select a Telephone Number or Telephone Number List to use as the primary Telephone Number in this Comms Path.
	Qualifier (When)	If required, select a Qualifier to define when this Telephone Number will be valid.
	Invert Qualifier	Select Invert Qualifier to enable the Telephone Number when the Qualifier is invalid.
	Second Telephone Number.	
	Telephone Number 2	Select a Telephone Number or Telephone Number List to use as the secondary Telephone Number in this Comms Path.
	Qualifier (When)	If required, select a Qualifier to define when this Telephone Number will be valid.
	Invert Qualifier	Select Invert Qualifier to enable the Telephone Number when the Qualifier is invalid.
	Maximum Online Time	Determines the maximum time that the Integriti Management Software is allowed to remain connected via this Modem Path.

	Maximum Dial Attempts	Determines the maximum dial attempts this Comms Task will use to contact the Integriti software. When the maximum attempts is reached, the Backup Task, if defined, will be triggered.
	RS232 Serial Interface Serial Channel None Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) Modem USB Slave USB Master IAC Onboard RS485	Select the Port that the Modem is connected to. No Modem connection. On-board "Port 0" connection. Unibus UART 1, RS232 Port 1 Unibus UART 1, RS232 Port 2 Unibus UART 2, RS232 Port 1 Unibus UART 2, RS232 Port 2 Unibus UART 3, RS232 Port 1 Unibus UART 3, RS232 Port 2 Unibus UART 4, RS232 Port 1 Unibus UART 4, RS232 Port 2
	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	
	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	
	Stop Bits 1 Bit 2 Bits	
	Modem Type PSTN GPRS	
	Modem Initialization String.	Enter a custom modem initialization string if required.

Options.	Permanent	Sets General Comms Task connection options. If selected, the Controller will try to reconnect with the Integrati Server if it becomes disconnected. i.e. The Controller will try to maintain a permanent connection. If this option is not selected, the Controller will only attempt one connection when the Comms Task is started.
	Temporary Comms Task	If selected, the Comms Task will be deleted upon completion of a communication session. e.g. When the Integrati Comms Task using a modem connection disconnects from the Integrati Server.
Advanced Options	Product Edition None Installer Professional	
	Encryption Key	Optional Site-based encryption key that is used with AES128 Private. Enter the 32 characters encryption key in HEXADECIMAL format.
	Encryption Pairing Code	A unique key generated for the connection between the Server and the Panel.
Miscellaneous Options	Encryption Type None AES128 AES128_Private	No encryption AES 128 AES 128 Private

<u>DIGITAL DIALLER FORMATS</u>		The Dialler format allows reporting via a range of Digital Dialler protocols.
Reporting	Dialler Format None IRFast Contact ID SIA Four Plus Two	Select Reporting Format for this Comms Task. No format. IR fast. Contact ID. SIA 4+2.
	Client Code	Determines the account code sent when reporting events to the Central Station. This is the default Client Code for this Comms Task which will be used if there is no Client Code programmed in the Area in which the event to report has occurred. If a Client Code has been programmed for an Area, then that Client Code will take precedence when events are reported for that Area. Options are provided to enter the Client Code in Hexadecimal and Decimal formats. Enter a Decimal value between 0 – 65535, or a Hexadecimal value between 0 – FFFF. Account Codes are typically provided by the Central Monitoring Station. The number of digits required will depend on the reporting format.
	Telephone Number 1 (Primary Telephone Number)	Use this setting to select the primary Telephone Number for this Comms Task if the Telephone number does not need to be qualified in any way. Note: If the Telephone Number needs to be Qualified, use the Telephone Number settings in the Advanced Options instead. A Telephone Number or Telephone Number List may be selected.
	Telephone Number 2 (Secondary Telephone Number)	Use this setting to select the secondary Telephone Number for this Comms Task if the Telephone number does not need to be qualified in any way. Note: If the Telephone Number needs to be Qualified, use the Telephone Number settings in the Advanced Options instead. A Telephone Number or Telephone Number List may be selected.

Advanced Settings	Comms Task Groups	Option to allow Input event reporting to be filtered based on the type of Input. Up to 16 separate Comms Task reporting Groups can be established. If one or more Groups are enabled in these options, an Input event will only be reported by this Comms Task if it has: - At least one matching Comms Task Group enabled in its associated Process Group. - No Comms Task Groups enabled in its associated Process Group. If no groups are enabled in these options, any Input events can be reported, regardless of how the Comms Task Group options have been set in the Input's Process Group.
	Primary Telephone Number. Telephone Number 1 Qualifier (When) Invert Qualifier	Allows the primary Telephone Number or Telephone Number List to be selected and paired with a Qualifier to define when it will be used. If a Qualifier is not required, use the Telephone Number settings in the Reporting Options instead. Select a Telephone Number or Telephone Number List to use as the primary Telephone Number in this Comms Task. If required, select a Qualifier to define when this Telephone Number will be valid. Select Invert Qualifier to enable the Telephone Number when the Qualifier is invalid.
	Secondary Telephone Number. Telephone Number 2 Qualifier (When) Invert Qualifier	Allows the secondary Telephone Number or Telephone Number List to be selected and paired with a Qualifier to define when it will be used. If a Qualifier is not required, use the Telephone Number settings in the Reporting Options instead. Select a Telephone Number or Telephone Number List to use as the secondary Telephone Number in this Comms Task. If required, select a Qualifier to define when this Telephone Number will be valid. Select Invert Qualifier to enable the Telephone Number when the Qualifier is invalid.
	Seize Action.	Select the Line Seize Action. The selected Entity will be controlled when the line is seized / unseized. <i>See Action Programming in “Generic Programming Operations” for details.</i>
	Pass Action	Select the Comms Pass Action. The selected Entity will be controlled when the dialler successfully sends a report to the Central Station. <i>See Action Programming in “Generic Programming Operations” for details.</i>

	Dialling options. Dial Decadic. Dumb Dial. Long Pace Dial.	Selects Pulse (“decadic”) dial when dialling, rather than tone (DTMF) dialing. Selects Dumb dialling. Normally the Comms Task will monitor the line for line faults, dial-tone, busy etc. and make dialling decisions accordingly. When Dumb dialling is selected, the Comms Task does not make “smart” decisions based on sensed tones. All tones sensed and dialer progress are still recorded to review. ???
	Handshake Wait Time (ms)	If required, program the time the task will wait for an initial handshake after dialling the Central Station.
	Acknowledgement Wait Time (ms)	The amount of time in milliSeconds that the Panel will wait for the Receiver to Acknowledge an alarm. If left set to 0, the default time of ??? will be used. NOT YET IMPLEMENTED
	Maximum Time until Backup Task (ms)	The maximum amount of time in milliSeconds before the Backup Comms Task will be triggered when the Primary Comms Task fails. If left set to 0, the default time of ??? will be used.
	Callback Telephone Number	Select a Telephone Number to use for the Callback function in this Comms Task.
	Client Telephone Number	Record the Panel’s telephone number here for reference.
IRFast Settings. (Only displayed if IRFast format selected)	Send Text. Send Contact ID. Send Time. C3K Compatible. 300 Baud. XMIT Info. Save time.	Send Review text for each event reported. Send an equivalent Contact ID string for each event reported, using the mapping option selected. This is useful when the automation system cannot understand native IRFast information. Send a text string of the Time/Date the event was recorded into review. The C3K Compatible Map is implemented for reporting Input events to Receivers and/or Automation Software that have not yet been updated for Integriti IRFast mapping. Forces all communications to 300 Baud instead of the default 1200 Baud. This need only be set if there are communication difficulties at 1200 Baud Send miscellaneous panel information before hanging up, including panel serial number, software version and security option settings. Causes the Receiver to Update the panel time and date from its system clock prior to hanging up. NOTE: An IRFast Receiver can set any of the above options to Yes on a per receiver basis. The above options should only be enabled upon instruction from the Central Station.

Contact ID Settings. (Only displayed if Contact ID format selected)	Contact ID Map	Select Contact ID Mapping for this Comms Task. Determines which zones are uniquely reported. <i>Refer to Contact ID Map documentation.</i>
	Standard	Standard Mapping oriented towards Intruder Alarm monitoring.
	Access	Access Mapping oriented towards Access Control with 2-Door Reader Modules.
	SIMS II	SIMS II Mapping for use with the SIMS II Central Station Automation Software. Allows all Inputs, on up to 35 Modules of every Module Type to be reported uniquely.
SIA Settings. (Only displayed if the SIA format selected)	Map	
	0 1 2	Hex digits are used for the Address field. Decimal digits will be used for the Address field. Not yet implemented. Note that if the Decimal Map option is selected, the address mapping alters and the maximum number of Modules of any one type is limited to 32. <i>See the Tables section of the rear of this manual for SIA address mapping.</i>
	RTC	If enabled, a time modifier (ti) prefixes every Event Data Code to provide the historical time stamp of the event. Note that this option may considerably slow down the rate of alarm transmission.
	ASCII	If enabled an ASCII text block is appended to the data to provide textual information from the system. NOTES: 1) This option may considerably slow down the rate of alarm transmission. 2) When this option is selected, the appropriate text for the first event will be sent in an ASCII block. Each subsequent event in the same phone call will only have ASCII text sent if it varies from the previous events. i.e. Only differences are sent to save on transmission time. 3) This option also has the effect of forcing one alarm event per packet. 4) With an opening/closing event, the following ASCII text may be appended if the related Area Communications options are selected. “Sys still open” At least one nominated System Area is Open (Off). “24Hr Partition” The 24 Hour (Tamper) part of the Area is Open (Off).
	Pident	
Options	Delayed Report Time	Enter a Delayed Report Time in Hours, Minutes and Seconds, if required. Determines the duration of delay when reporting alarms to the Central Station.
	Look Ahead.	New Alarm events will be reported ahead of multi-break reports on Inputs that have already been reported.
	General Open/Close.	Area Open/Close reporting will only be done on the 1 st Area to Open and the last Area to Close, with the exception of Areas with the “Not General Area” option enabled.
	Xmit Isolated.	???
	Maximum Online Time (ms)	Program the maximum online time in milliSeconds.

	Maximum Events to send per call.	Program the maximum number of events allowed to be reported per call.
	Maximum Dial Attempts	Determines the maximum dial attempts this Comms Task will use to contact the Central Station.
Event Filtering	Event Filter	
	Report Options	
	Area Filter	

GSM Comms Task Notes

- The format (IRfast or ContactID) used to communicate the normal event data to the FE3000 is determined by the FE3000. If the FE3000 tells the GSM Comms Task to use IRfast, then IRfast is what the GSM Comms Task sends. Note that the new Integriti IRfast may not be implemented in the Central Monitoring Station whereas the C3K IRfast may be. An option is provided for “C3k compatible IRfast” data to be sent.
- There is currently no option in the Comms Task to disable SMS control commands. Restricting SMS control of an entity is achieved via the User’s Menu Group.
- When GSM Comms Task is configured as a Backup Comms Task, under normal “idle” conditions, no events are reported but SMS control messages are still processed.
- See information following the GSM Comms Task programming for full details of the SMS Command feature.

<u>GSM FORMAT</u>		The GSM format allows primary or backup reporting via compatible Fratech Multipath IP STU or FE3000 products. It is used to communicate reportable events to a Central Monitoring Station, to send reportable events via SMS message and/or to receive SMS control messages.
Connectivity	RS232 Serial Interface Serial Channel None Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) USB Master USB Slave IAC Onboard RS485 Modem	Select the Port that the Modem is connected to. GSM Format utilizes the following connection options: 1) “Uart 0” with Cable P/N: 996790 Integrity Port 0 to Multipath IP Interface Cable. 2) UniBus UART RS232 Port with Cable P/N: 994092 Serial Interface Cable. No Modem connection. On-board “Port 0” connection. Unibus UART 1, RS232 Port 1 Unibus UART 1, RS232 Port 2 Unibus UART 2, RS232 Port 1 Unibus UART 2, RS232 Port 2 Unibus UART 3, RS232 Port 1 Unibus UART 3, RS232 Port 2 Unibus UART 4, RS232 Port 1 Unibus UART 4, RS232 Port 2 Not relevant to this format. Not relevant to this format. Not relevant to this format. Not relevant to this format.

	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	The next four options configure the serial port. The recommended port configuration for communications between the Integriti Controller and an FE3000 is: • 1200 baud • 8 Bits • No Parity • 1 Stop Bit
	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	
	Stop Bits 1 Bit 2 Bits	
Reporting	Client Code	Determines the account code sent when reporting events to the Central Station. This is the default Client Code for this Comms Task which will be used if there is no Client Code programmed in the Area in which the event to report has occurred. If a Client Code has been programmed for an Area, then that Client Code will take precedence when events are reported for that Area. Options are provided to enter the Client Code in Hexadecimal and Decimal formats. Enter a Decimal value between 0 – 65535, or a Hexadecimal value between 0 – FFFF. Account Codes are typically provided by the Central Monitoring Station. The number of digits required will depend on the reporting format.
	SMS Number 1 (Primary SMS Telephone Number)	Use this setting to select the primary Telephone Number for this Comms Task if the Telephone number does not need to be qualified in any way. Note: If the Telephone Number needs to be Qualified, use the Telephone Number settings in the Advanced Options instead. A Telephone Number or Telephone Number List may be selected.

	SMS Number 2 (Secondary SMS Telephone Number)	Use this setting to select the secondary Telephone Number for this Comms Task if the Telephone number does not need to be qualified in any way. Note: If the Telephone Number needs to be Qualified, use the Telephone Number settings in the Advanced Options instead. A Telephone Number or Telephone Number List may be selected.
	General Reporting Options Enable SMS. Enable Alarms. Xmit Isolated	When this option is set, the Comms Task waits for an event to transfer to the FE3000. When an event is detected it is sent to the FE3000 to be reported to the nominated SMS Telephone Number or Telephone Number List as an SMS Text message. The FE3000 will attempt to send the SMS message and will report back whether or not it was successful. If the FE3000 could not successfully send the message, no further action is taken by the GSM Comms Task. When there is an SMS message pending to be sent, if the FE3000 takes longer than 30 seconds to be free to accept the next SMS message then the pending SMS message will be discarded. When this option is set, the Comms Task waits for an event to transfer to the FE3000. When an event is detected it is sent to the FE3000 to be reported to the Central Monitoring Station. The FE3000 will attempt to report the event via one of its many communication paths. The FE3000 reports back whether or not it was successful with its attempt to communicate the event(s). If the FE3000 could not successfully communicate the event(s) to the Monitoring Station then the GSM Comms Task can pass the event(s) to its programmed Backup Comms Task. Enabling the “Xmit Isolated” option forces the Comms Task to report all events on isolated Inputs. Normally, if an event for an Input is about to be reported and the Input is then isolated, then the reporting of that event is skipped. E.g. If there are many events queued up to report for an Input and then the Input is isolated, the remaining events in the queue for that Input will not be reported, allowing new events to be reported sooner.

Options	Send IRfast. Use C3K Compatible IRFast. Update Time. Save RSSI Alarm Look Ahead. SMS Look Ahead. General Opening / Closing. Need PIN SMS Error Reply. Maximum Messages	IRfast data will be sent instead of Contact ID. Concept 3000 compatible IRfast mapping allows compatibility with Automation Software that has not yet been updated for Integriti IRfast format. The Control Module's Real-time clock will be updated from the FE3000 status packet every hour on the hour. Save RSSI information to Review allows the Received Signal Strength Information to be logged to Review. New alarms will be reported ahead of multi-break messages for Inputs that have already reported. New SMS alarm messages will be reported ahead of multi-break messages for Inputs that have already reported. Whenever all Areas that are programmed to report Open/Close are turned On, a general Area close is reported. As soon as the first Area is turned Off, a general Area open is reported. In Area Programming, some Areas can be nominated to be ignored in the general Area calculation allowing them to still be reported individually. A PIN Code is required to be sent with SMS commands. If SMS commands are received that result in some sort of error (e.g. Command Syntax, Permissions deny control, etc.) then this option allows an error reply to be sent back to the Sender. Maximum SMS messages allowed to be sent in a 60 second period. Note that messages will bank up if they are occurring faster than this rate. The default setting of 0 means that the maximum messages will be 10 per 60 seconds.
Contact ID	Contact ID Map Standard Access SIMS II	Select Contact ID Mapping for this Comms Task. Determines which zones are uniquely reported. <i>Refer to Contact ID Map documentation.</i> Standard Mapping oriented towards Intruder Alarm monitoring. Access Mapping oriented towards Access Control with 2-Door Reader Modules. SIMS II Mapping for use with the SIMS II Central Station Automation Software. Allows all Inputs, on up to 35 Modules of every Module Type to be reported uniquely.
Advanced Settings	Comms Task Groups	Option to allow Input event reporting to be filtered based on the type of Input. Up to 16 separate Comms Task reporting Groups can be established. If one or more Groups are enabled in these options, an Input event will only be reported by this Comms Task if it has: - At least one matching Comms Task Group enabled in its associated Process Group. - No Comms Task Groups enabled in its associated Process Group. If no groups are enabled in these options, any Input events can be reported, regardless of how the Comms Task Group options have been set in the Input's Process Group.

	First SMS Number. SMS Number 1 Qualifier (When) Invert Qualifier	Select a Telephone Number or Telephone Number List to use as the primary Telephone Number in this Comms Task. If required, select a Qualifier to define when this Telephone Number will be valid. Select Invert Qualifier to enable the Telephone Number when the Qualifier is invalid.
	Second SMS Number. SMS Number 2 Qualifier (When) Invert Qualifier	Select a Telephone Number or Telephone Number List to use as the secondary Telephone Number in this Comms Task. If required, select a Qualifier to define when this Telephone Number will be valid. Select Invert Qualifier to enable the Telephone Number when the Qualifier is invalid.
	CID Telephone Number	Select a Telephone Number to use for reporting to a Central Station Digital Receiver.
	Service Telephone Number	Select a Telephone Number for the SMS service centre. This number can be obtained from the Network you subscribe to and is mandatory for any SMS operations.
	SMS Control Number	Select a Telephone Number to define a number that is allowed to perform SMS Control operations if the “Need PIN” option is not enabled.
	Status monitoring GSM Reg Input. GSM Signal Input GSM Fail Input GSM Backup Input GSM Online Input	Allows Inputs to be specified for monitoring a number of GSM Comms Task states. Unused Zone Inputs can be assigned to these functions. Any Zones used for this purpose should have the “Ignore Physical” option enabled. This Zone will indicate changes in the state of the GSM modem registration. The Input is alarmed when the modem de-registers and sealed when the modem re-registers. This Zone will be put into Alarm when the FE3000 reports to the Integriti Controller that it has low signal strength. The Zone will restore when the FE3000 reports that the signal strength is satisfactory. This Zone is will be put into Alarm when some error conditions occur between the Integriti Controller and the FE3000. This Zone will indicate when the Backup Comms Task is Triggered. This Zone will be Sealed when communications with the FE3000 are working and in Alarm when they are not.

SMS Control

The GSM Comms Task can be used to turn Areas on/off, turn Auxiliaries on/off and to trigger Named Actions via SMS control commands. Inputs can also be Isolated or de-Isolated. The GSM Comms Task can be configured to authenticate an SMS command either via a Telephone Number or via a User PIN.

If only the Telephone Number is used as the authentication method then there is no restrictions applied to the SMS control command. This means that as long as the command syntax is correct the SMS control action is carried out (E.g. any Area can be turned ON/OFF or any Input can be Isolated/de-Isolated etc.).

If a User PIN is provided as part of the SMS control command then the User's permissions governs the level of control that the SMS control command can execute. If the User does not have access to control the entity type in their Remote Access Permissions of their Menu Group, then they cannot control the entity. Some SMS control commands also have additional checks, for example:

- When controlling an Area ON the User must have the Area in their "Area ON List".
- When controlling an Area OFF the User must have the Area in their "Area OFF List".
- When Isolating or De-Isolating an Input the User must have the Input in their "Area OFF List".
- When triggering a Named Action, if the Named Action has an "Action Group" set then the User must have at least one matching "Action Group" set to that of the Named Action.

When a valid SMS control command has been received and processed, an SMS reply will be sent back to the original SMS phone number. In most cases the SMS reply will be the review associated with the action that was performed, however in some circumstances an error reply may be sent or even no reply will be sent.

Examples of these exceptions are:

- SMS Alarms are being sent instead of SMS replies (SMS Alarms are a higher priority than SMS replies)
- The review for the executed action was not detected or the FE3000 was full and unable to accept additional SMS messages.

As with SMS Alarms, if there is an SMS reply message pending to be sent and the FE3000 takes longer than 30 seconds to be free, then the pending SMS reply message will be discarded.

See the following table for the command set.

SMS Control Command Syntax

Command Syntax	Command Description
[<PIN>] ?	Display SMS Help
[<PIN>] A <Area ID> <N/F>	Control an Area using its ID
[<PIN>] A <Area Name> <N/F>	Control an Area using its Name
[<PIN>] A <Area ID> L	List 4 Area Names starting at Area ID
[<PIN>] A <Area Name> L	List 4 Area Names starting at Area Name
[<PIN>] A ?	Display Area Help
[<PIN>] I <Input Address> <I/D>	Isolate an Input using its ID
[<PIN>] I <Input Name> <I/D>	Isolate an Input using its Name
[<PIN>] I <Input ID> <L>	List 4 Input Names starting at Input ID
[<PIN>] I <Input Name> <L>	List 4 Input Names starting at Input Name
[<PIN>] I ?	Display Isolate Help
[<PIN>] P <Named Action Address> <N/F>	Trigger a Named Action using its ID
[<PIN>] P <Named Action Name> <N/F>	Trigger a Named Action using its Name
[<PIN>] P <Named Action ID> <L>	List 4 Named Actions starting at Named Action ID
[<PIN>] P <Named Action Name> <L>	List 4 Named Actions starting at Named Action Name
[<PIN>] P ?	Display Named Action Help
[<PIN>] X <AUX Address> <N/F>	Control an Auxiliary using its ID
[<PIN>] X <AUX Name> <N/F>	Control an Auxiliary using its Name
[<PIN>] X <AUX ID> <L>	List 4 Auxiliary Names starting at Auxiliary ID
[<PIN>] X <AUX Name> <L>	List 4 Auxiliary Names starting at Auxiliary Name
[<PIN>] X ?	Display Auxiliary Help
[<PIN>] R	Reset the SMS buffer to the latest review
[<PIN>] R ?	Display Reset SMS Help

Example SMS Control commands

Example	Example Description
01?	01=User PIN, ?=Display the SMS Help message
01A001N	01=User PIN, A=Area Control, 001=Area #001, N=Turn ON
AHouseF	A=Area Control, House=Area Name, N=Turn OFF
A1L	A=Area Control, 1=Area #1, L=List 4 Area Names starting at 1
AHouseL	A=Area Control, 1=Area #1, L=List 4 Area Names starting at House
A?	A=Area Control, ?=Display the Area Help message
01IC01:Z05I	01=User PIN, I=Isolate Control, C01:Z05=Input C01:Z05, I=Isolate
IEntry PIRD	I=Isolate Control, Entry PIR=Input (E.g. C01:Z05), D=Delsolate
IC01:Z05L	I=Isolate Control, C01:Z05=Input C01:Z05, L=List 4 Input Names starting at C01:Z05
IEntry PIRL	I=Isolate Control, Entry PIR=Input (E.g. C01:Z05), L=List 4 Input Names starting at Entry PIR
I?	I=Isolate Control, ?=Display the Isolate Help message
01P001N	01=User PIN, P=Named Action Control, 001=Named Action #001, N=Trigger ON
PUnlockF	P=Named Action Control, Unlock=Named Action Name, F=Trigger OFF
P1L	P=Named Action Control, 1=Named Action #1, L=List 4 Named Action Names starting at 1
PUnlockL	P=Named Action Control, Unlock=Named Action Name, L=List 4 Named Action Names starting at Unlock
P?	P=Named Action Control, ?=Display the Named Action Help message
01XC01:X07N	01=User PIN, X=Auxiliary Control, C01:X07=Auxiliary C01:X07, N=ON
XStrobeF	X=Auxiliary Control, Strobe=Auxiliary (E.g. C01:X07), F=OFF
XC01:X07L	X=Auxiliary Control, C01:X07=Auxiliary C01:X07, L=List 4 Auxiliary Names starting at C01:X07
XStrobeL	X=Auxiliary Control, Strobe=Auxiliary (E.g. C01:X07), L=List 4 Auxiliary Names starting at Strobe
X?	X=Auxiliary Control, ?=Display the Auxiliary Help message
01R	01=User PIN, R=Reset SMS command
R?	R=Reset SMS, ?=Display the Reset SMS Help message

<u>AUTOMATION FORMAT</u>	NOTE: All letters in valid commands sent to the Automation Comms Task must be uppercase only.	The “Automation” communication format allows the Integrity Controller to connect to a 3rd party Home/Building Automation system via an RS232 Serial or Ethernet connection. The protocol is ASCII based for ease of use and is designed primarily to enable home automation or building management system (BMS) connectivity.
Filtering	Review Filter	The Review Filter allows up to 5 Entities to be selected to restrict the system entities that are sent via the Automation Comms Task Review streaming. e.g. Area List, Auxiliary List, etc.
	Comms Task Groups	Option to allow Input event reporting to be filtered based on the type of Input. Up to 16 separate Comms Task reporting Groups can be established. If one or more Groups are enabled in these options, an Input event will only be reported by this Comms Task if it has: - At least one matching Comms Task Group enabled in its associated Process Group. - No Comms Task Groups enabled in its associated Process Group. If no groups are enabled in these options, any Input events can be reported, regardless of how the Comms Task Group options have been set in the Input’s Process Group.
	Review Level Everyone User - Essential User - Standard User - Detailed Installer - Standard Installer - Detailed Inner Range - Debug	Select the Review Level required to be output for this Automation Comms Task. This option determines the amount of detail that will be included in the Review log. Lowest Level of detail. Most detailed Level.
	General Filter options EN Review Historic Review	The Automation Comms Task will use the EN review buffer (if present) rather than the standard review buffer. This option is only relevant if the “EN 50131” Controller option has been enabled. If this option is enabled, then instead of simply sending live review from the time at which the Automation Comms Task was started, The Comms Task will send all review in the review buffer (could be up to 100,000 events) starting with the oldest event. If the Comms Task remains enabled, then when all historical review has been sent, it will switch to live review. Note that if the Comms Task is restarted and this option is enabled, it will send all historical review again.

Connectivity	RS232 Serial Interface Serial Channel None Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) Modem USB Slave USB Master IAC Onboard RS485	Select the Port that the Automation Comms Task will use. No connection. On-board "Port 0" connection. Unibus UART 1, Port 1 Unibus UART 1, Port 2 Unibus UART 2, Port 1 Unibus UART 2, Port 2 Unibus UART 3, Port 1 Unibus UART 3, Port 2 Unibus UART 4, Port 1 Unibus UART 4, Port 2 Not relevant to this format. Appears as a Virtual Comm Port in Windows and may be used for this format. Not relevant to this format. Not relevant to this format.
	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	
	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	
	Stop Bits 1 Bit 2 Bits	
Timing	Poll Time	Sets the maximum time allowed between received packets before the Automation Comms Task considers the link to have failed and triggers the "Online Input". Programmed in Hours, Minutes and Seconds. Maximum Poll Time that can be programmed is ???

	Pacing Time	Adjusts the rate at which Historic Review events are output when the communications link is re-established. Programmed in Minutes and Seconds. Maximum Pacing Time that can be programmed is ???
	Repeat Time	If the “Acknowledge Review” option has been selected, then for each review event sent, an acknowledge packet must be received before advancing to the next event. If an acknowledge is not received within 5 seconds, the event will be resent after waiting out the Repeat time. The Repeat Time is programmed in Hours, Minutes and Seconds. Maximum Repeat Time that can be programmed is ???
Ethernet Connection	Server IP Address	View or Enter the IP Address of the Server PC.
	TCP Port	View or Enter the Server TCP Port Number. The default Port number does not normally need to be changed.
	Server Host Name	Select required DNS Server Name. DNS Servers are programmed separately.
	TCP Mode None Server Client	
	Retries	
	Connection Timeout	Programmed in Minutes and Seconds. Maximum time that can be programmed is ???
	Connection Attempt Timeout	Programmed in Minutes and Seconds. Maximum time that can be programmed is ???
Output Options	Header Format Tstamp DateTime Sequence LCD Sequence LCD DateTime Sequence DateTime	Select the option for the Review Header format. Timestamp only. Date and Time only. Sequence Number only. (Event ID) LCD ? and Sequence Number. LCD ? and Date/Time Sequence Number and Date/Time

	Body Format Raw Full Text LCD Full Text LCD Abbrev Text	Select the option for the Review Body format. Only Raw Hexadecimal Review data will be output after the Event ID. No text will be output. ? ? Review events will be sent in an abbreviated form. Any relevant entity names (if programmed) will be replaced with the entity ID. e.g. Normal Review log entry: Auto Comms Task O/P: Alarm on Roller Door Reed in Garage Alarm C01:Z15
Flags	Transfer Checksum Receive Checksum Send Review Acknowledge Review All Review	Insert a checksum field in all transmissions. A checksum field comprises a “~” character followed by two hexadecimal digits inserted just prior to the end of frame character “}”. The Automation Comms Task will expect a checksum field in all received packets, and will reject any packet that has a bad checksum. Enables Review streaming output. The Automation Comms Task will expect an acknowledge message to be returned following each Review event sent. If enabled, all Review filtering will be ignored.
Review Options	No DOS-Style Line Breaks LCD Year No Headers Or Braces in Review	
Miscellaneous Options	Online Input	Select an Input to be used to monitor the Online status of the Automation Comms Task communications link. An unused Zone Input can be assigned to this function. Any Zone used for this purpose should have the “Ignore Physical” option enabled.

<u>EMS FORMAT</u>		The “EMS” communication format allows the Integriti Controller to provide a high-level connection to an Elevator Management System via an RS232 Serial or Ethernet connection. “Lift Groups” must also be programmed to support this feature. The Integriti Controller lift interface allows for one type of lift interface per controller. If a high-level interface is used, only one EMS Comms Task is allowed per Integriti Controller.
Connectivity	RS232 Serial Interface Serial Channel None Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) Modem USB Slave USB Master IAC Onboard RS485	Select the Port that the Automation Comms Task will use. No Modem connection. On-board “Port 0” connection. Unibus UART 1, Port 1 Unibus UART 1, Port 2 Unibus UART 2, Port 1 Unibus UART 2, Port 2 Unibus UART 3, Port 1 Unibus UART 3, Port 2 Unibus UART 4, Port 1 Unibus UART 4, Port 2 Not relevant to this format. ? Not relevant to this format. Not relevant to this format.
	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	
	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	
	Stop Bits 1 Bit 2 Bits	

Primary Ethernet Connection	Primary Server IP Address	View or Enter the IP Address of the Server PC.
	Primary TCP Port	View or Enter the Server TCP Port Number. The default Port number does not normally need to be changed.
	Primary Server Host Name	Select required DNS Server Name. DNS Servers are programmed separately.
	Primary TCP Mode None Server Client	 Normally left set to None.
	Primary Retries	Programmed if “Client” TCP mode selected above.
	Primary Connection Timeout	Programmed in Minutes and Seconds. Maximum time that can be programmed is ??? NOT YET IMPLEMENTED.
	Primary Connection Attempt Timeout	Programmed in Minutes and Seconds. Maximum time that can be programmed is ??? NOT YET IMPLEMENTED.
Secondary Ethernet Connection	Secondary Server IP Address	View or Enter the IP Address of the Server PC.
	Secondary TCP Port	View or Enter the Server TCP Port Number. The default Port number does not normally need to be changed.
	Secondary Server Host Name	Select required DNS Server Name. DNS Servers are programmed separately.
	Secondary TCP Mode None Server Client	??? Normally left at None?
	Secondary Retries	Programmed if “Client” TCP mode selected above.
	Secondary Connection Timeout	Programmed in Minutes and Seconds. Maximum time that can be programmed is ??? NOT YET IMPLEMENTED.

	Secondary Connection Attempt Timeout	Programmed in Minutes and Seconds. Maximum time that can be programmed is ??? NOT YET IMPLEMENTED.
Miscellaneous Options	Online Input Protocol None Kone IP Kone RS232 Otis RS232 Thyssen RS232	Select an Input to be used to monitor the Online status of the EMS Comms Task communications link. An unused Zone Input can be assigned to this function. Any Zone used for this purpose should have the “Ignore Physical” option enabled. Select the EMS communications Protocol for this EMS Comms Task. No protocol selected. Kone HLI Access Control Protocol V2.6. Kone Access Control Protocol Rev 1.5. Otis RS-232 Thyssen Krupp Destination Selection Control (DSC) version 1.0.

Introduction to Securitel Comms Task.

The Securitel format allows connection to 3rd party communicators that use the Securitel Serial protocol as the interface.

The Securitel network that the protocol was originally developed for is no longer in operation, but the protocol is still used in Australia by Subscriber Terminal Units (STUs) to report via communications paths such as GSM, GPRS or IP.

The Securitel network was a “direct-line” alarm transmission network that was supplied and maintained by Telstra Australia. Alarm panels in the field were connected to a Subscriber Terminal Unit (a STU) and the STU would communicate events via the PSTN to Nodes that were hosted by Telstra. These events were then transmitted to a Central Monitoring Station for processing/actioning.

The Alarm panel communicates to the STU via the Securitel communication protocol. The Securitel protocol allows for either Channel/PIN data or Serial data.

The Integriti Securitel format uses Serial data. When an Alarm panel is reporting Serial data to the STU, the event description from the Alarm panel to the STU can describe:

- 255 Inputs being in one of the following states
 - Priority1
 - Priority2
 - Priority3
 - Tamper
 - Trouble
 - Man. Isolate
 - Auto Isolate
- Area 1 to 31 being Open or Close
- General Area Open or Close
- A few other miscellaneous events.

An Integrity Controller can support thousands of Inputs and the STU can only accept an Input number from 1 to 255, so the Securitel Comms Task has the job of collating many Inputs together in an attempt to end up with meaningful event information at the Central Monitoring Station.

See the “Integriti Securitel Comms Task Input Map” document for details.

The Securitel Comms Task also has another collation mechanism that is on a per Area basis. Each time that an Input in an Area reports a new Alarm, Tamper or Isolate, an additional Area Alarm, Area Tamper or Area Isolate can also be generated. When the Area is eventually disarmed, an Area Alarm Restore, Area Tamper Restore or Area Isolate Restore is generated (one Restore event per event type that was reported during this arming cycle).

The Securitel Comms Task has options to report Input events, Area events or both.

When multiple inputs across multiple modules are collated the reporting logic is as follows:

1. If a new input event (E.g. an Alarm) is being reported then the appropriate Securitel Input Number is looked up and the event is sent to the STU.
2. If a new input restore (E.g. going from Alarm to Seal) is being reported, look up all of the other module's inputs of the same type that the Securitel Input Number is collated with. If all of the inputs found are sealed then the restore event is sent to the STU. If an input(s) is unsealed then when the last input seals then the restore event is sent to the STU.

e.g. There are 4 Expander modules and 1 RF module on the Integriti Controller. Expander 2 has a Cabinet Tamper event, this is reported to the STU immediately. Then Expander 3 has a Cabinet Tamper event, this is reported to the STU immediately. Then Expander 3 has a Cabinet Tamper restore, this is not reported to the STU because Expander 2 still has its Cabinet Tamper unsealed. Expander 2 has a Cabinet Tamper restore and this is reported to the STU indicating that all Expander module Cabinet Tamper inputs are sealed.

<u>SECURITEL FORMAT</u>	Australia Only.	
Connectivity	RS232 Serial Interface Serial Channel None Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) Modem USB Slave USB Master IAC Onboard RS485	Select the RS-232 Port that the STU is connected to. No Modem connection. On-board "Port 0" connection. Unibus UART 1, RS232 Port 1 Unibus UART 1, RS232 Port 2 Unibus UART 2, RS232 Port 1 Unibus UART 2, RS232 Port 2 Unibus UART 3, RS232 Port 1 Unibus UART 3, RS232 Port 2 Unibus UART 4, RS232 Port 1 Unibus UART 4, RS232 Port 2 Not relevant to this format. Not relevant to this format. Not relevant to this format. Not relevant to this format.
	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	STUs using the Securitel Communications Protocol are generally capable of communicating to Alarm panels at 300, 1200 or 9600 Baud. The recommended Baud Rate for communications between the Integriti Controller and a STU is 1200 Baud; however, you should check the Installation and/or Configuration information supplied with the STU to ensure a compatible Baud rate is chosen.
	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	The recommended number of Data Bits for communications between the Integriti Controller and a STU is 8. Check the Installation and/or Configuration information supplied with the STU to ensure a compatible option is chosen.

	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	The recommended Parity for communications between the Integriti Controller and a STU is None. Check the Installation and/or Configuration information supplied with the STU to ensure a compatible option is chosen.
	Stop Bits 1 Bit 2 Bits	The recommended number of Stop Bits for communications between the Integriti Controller and a STU is 1. Check the Installation and/or Configuration information supplied with the STU to ensure a compatible option is chosen.
Advanced Settings	Comms Task Groups	Option to allow Input event reporting to be filtered based on the type of Input. Up to 16 separate Comms Task reporting Groups can be established. If one or more Groups are enabled in these options, an Input event will only be reported by this Comms Task if it has: - At least one matching Comms Task Group enabled in its associated Process Group. - No Comms Task Groups enabled in its associated Process Group. If no groups are enabled in these options, any Input events can be reported, regardless of how the Comms Task Group options have been set in the Input's Process Group.
Options	General Open/Close. Don't Report Area Events. Don't Report Input Events	Area Open/Close reporting will only be done on the 1st Area to Open and the last Area to Close, with the exception of Areas with the "Not General Area" option enabled. Area Open/Close events will not be sent by this Comms Task. Input Events will not be sent by this Comms Task.
Miscellaneous Settings	Auxiliary Action Hard ID Online Input	Selects the system Entity to be controlled by the Securitel Command-back Auxiliary. Sets the Securitel Hard ID to be used for this Comms Task. The Hard ID is the Securitel equivalent to the client code used in other formats and is programmable in HEX from 0001 to FFFF. The Hard ID is provided by the Central Monitoring Station. Note that while the Hard ID is a HEX number, the number provided by the Cenral Station will normally only contain Decimal characters. Simply enter the number as it is provided by the Central Station. The "Multiple Area Client Code" option has no effect when selected for securitel. The Hard ID programmed here is always used. Select an Input to be used to monitor the Online status of the Securitel Comms Task communications link. An unused Zone Input can be assigned to this function. Any Zone used for this purpose should have the "Ignore Physical" option enabled.

Introduction to the Intercom Comms Task.

The Integriti Controller has an Intercom Comms Task to provide a high-level interface to a 3rd party Intercom system. The Integriti system also has an Apartment entity. These features provide an interface that allows an Apartment to grant access to a Call Location.

An Apartment can optionally have a Floor defined as well as having an Intercom System Floor and an Intercom System Unit. Up to 32 Call Locations can be defined in the Intercom Comms Task and each can optionally have a Door and/or up to 4 Lift Cars defined.

When the Intercom Comms Task detects that an Apartment has granted access to a Call Location, the defined Door and Lift(s) are temporarily unlocked/unsecured to allow access.

At present, the Intercom Comms Task only supports the Kenwei Intercom system. A brief description of the Kenwei system is provided after the Intercom Format programming details.

<u>INTERCOM FORMAT</u>		The Intercom format allows connection to 3 rd party Intercom products to allow access control operations to be performed from an Intercom Terminal.
Connectivity	RS232 Serial Interface Serial Channel None Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) Modem USB Slave USB Master IAC Onboard RS485	Select the Port that the Modem is connected to. No connection. On-board "Port 0" connection. Unibus UART 1, Port 1 Unibus UART 1, Port 2 Unibus UART 2, Port 1 Unibus UART 2, Port 2 Unibus UART 3, Port 1 Unibus UART 3, Port 2 Unibus UART 4, Port 1 Unibus UART 4, Port 2 Not relevant to this format. Not relevant to this format. Not relevant to this format. ? Kenwei: The Kenwei Intercom can be connected to an Integriti Controller: • Via Port 0 or a UniBus RS-232 Port using an RS485-RS232 Protocol Converter. • Directly to an Integriti Controller RS-485UniBus Port.
	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	Select the Baud Rate for the connection to the Intecom system. Kenwei: 9600 Baud.

	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	Select the number of Bits for the connection to the Intecom system. Kenwei: 8.
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	Select the Parity for the connection to the Intecom system. Kenwei: None
	Stop Bits 1 Bit 2 Bits	Select the number of Stop Bits for the connection to the Intecom system. Kenwei: 1
Miscellaneous Settings	Intercom Type Kenwei	Selects the type of Intercom to be connected.
	Door / Lift Mappings Door to Unlock Lift 1 to Desecure Lift 2 to Desecure Lift 3 to Desecure Lift 4 to Desecure	Each Intercom Call Location can be mapped to a Door and/or up to 4 Lifts to allow the nominated Door to be temporarily unlocked and/or the nominated Lift/s to be temporarily De-secured. The Unlock and De-secure times are programmable specifically for this Comms Task. <i>See below.</i> Up to 32 Call Locations can be programmed.
	Door Time	Program the Door Unlock Time. This option applies to all Doors controlled by this Comms Task. If left at 0, the Unlock Time setting in the Door programming will be used.
	Floor Time	Program the Floor Button (De-secure) Time. This option applies to all Floors controlled by this Comms Task. If left at 0, the Button Time setting in the Lift programming will be used.

Intercom Comms Task Kenwei Interface.

Description of the Kenwei Intercom system:

The Kenwei Intercom system consists of Indoor Monitor units and Outdoor Camera units. Distributor modules are used to connect the Indoor and Outdoor units.

The standard Distributor module has a DIP switch that is used as the Floor selection for the Kenwei Intercom system and allows for up to 4 Indoor Monitor units connected to a single Distributor module. There is also a special type of Distributor module that allows for up to 4 Outdoor Camera unit connections. Distributor modules can be connected in series to build up the intercom system to the required size for the installation.

The Kenwei Intercom system addresses the Indoor Monitor units via the Distributor module's Floor and then the terminal location.

e.g. If the Distributor module was set to Floor 17 and the Indoor Monitor was connected to terminal location 3, the Indoor Monitor's address would be 1703.

The Kenwei Intercom system addresses the Outdoor Camera unit as number 1 when it is connected directly to a Distributor module or via the terminal location when connected to a special Outdoor Camera Distributor module.

e.g. If the Outdoor Camera unit was connected to terminal location 3 of an Outdoor Distributor module, the Outdoor Camera's address would be 3.

Refer to the Kenwei Installation manual for full details.

Interface between Integriti and the Kenwei Intercom system:

The Integriti Apartment's Intercom System Floor and an Intercom System Unit equate to Kenwei's Floor and terminal location of an Indoor Monitor unit. The Integriti Intercom Comms Task's Call Location equates to Kenwei's Outdoor Camera address. The Kenwei Intercom system's RS485 LAN communication protocol has been provided to Inner Range. The Kenwei communication traffic is watched for an "unlock the door" command being sent from an Indoor Monitor unit to an Outdoor Camera unit. When this unlock command is observed, the Integriti Intercom Comms Task searches for an Apartment that matches the Kenwei Indoor Monitor's address. If a match is found the defined Door and/or Lift(s) are temporarily unlocked/unsecured to allow access as well as logging an event to review. If no Apartment is found to match the Kenwei unlock command, then only review is logged.

The Kenwei Intercom's communication traffic is watched by connecting to a segment of the Kenwei RS485 LAN (between the serial Distributors) to a UART on the Integriti Controller. During development/testing this was achieved via an RS485 to RS232 cable connected to UART Port0. The port configuration that is required is 9600,N,8,1 (as per the Figure 2).

Limitations of the Integriti to Kenwei interface:

A typical standalone installation of a Kenwei Intercom system involves a physical electronic lock and/or a lamp to be directly wired to the Kenwei Outdoor Camera unit. There are 3 ways that access through the door can be granted: via the Indoor Monitor unit, via a key fob access at the Outdoor Camera unit and via a PIN password entry at the Outdoor Camera unit. Key fobs are registered with and PINs are saved to an Outdoor Camera unit.

Using the Kenwei key fob or PIN access from the Outdoor Camera unit cannot be used when using the Integriti to Kenwei interface. This means that the only method to grant access to the Door/Lift(s) is from an Indoor Monitor unit.

To overcome this limitation it would be envisioned that an Integriti access control Reader would be installed alongside the Kenwei Outdoor Camera unit.

<u>SKY TUNNEL FORMAT</u>		
Connectivity		

Telephone Numbers

Entity/Feature	Option	Description
Telephone Numbers		Select Telephone Number to program.
Name.		Program a name for the Telephone Number up to 32 characters in length.
Miscellaneous Options		Enter the Telephone Number. Some Telephone Numbers such as the SMS Service number must be entered in international format starting with the country code. e.g. The Telstra Australia SMS service number is entered as "61418706700".

Network Interface Controllers

Entity/Feature	Option	Description
Network Interface Controllers		Select Network Interface to program.
IP Address	Local IP Address	000.000.000.000
	Subnet Mask	000.000.000.000
	Gateway address	255.255.255.000
	Use DHCP	000.000.000.000
DNS Settings	Primary DNS	000.000.000.000
	Secondary DNS	

DNS Servers

Entity/Feature	Option	Description
Network Interface Controllers		Select Network Interface to program.
IP Address	Local IP Address	000.000.000.000

System Options Programming

Entity/Feature	Option	Description
Memory Options		Select a Memory Configuration. (Not currently used)
Auxiliary Options		Program/Edit Auxiliary options.
EOL Configurations		Program/Edit Zone Input End Of Line Resistor Schemes.

Memory Configuration

Entity/Feature	Option	Description
Select Configuration		Not currently used.

Auxiliary Options

Entity/Feature	Option	Description
Auxiliary to Edit		Select the Auxiliary to program or edit.
Auxiliary Name		Program a text name of up to 32 characters in length. The name may include the Auxiliary location and/or function.
Options	Auxiliary Options. No Review. Allow Turn On on Reset.	Activity on this Auxiliary will not be saved to Review. On a System Reset, the Auxiliary will be returned to the state it was in prior to the reset.
	Analogue Calibration	Assign a Calibration to this Auxiliary. Determines the calibration parameters for this Auxiliary if it is an Analogue output type. Calibrations are programmed separately.

EOL Configurations

Entity/Feature	Option	Description
EOL Configuration		Select the EOL Configuration to program or edit.. CAUTION: Do not edit the default EOL configurations or create new configurations without a thorough understanding of how the scheme operates, and the ramifications across your system. Note that most legacy Concept Module do not support alternate EOL schemes.
Name		Program a text name of up to 32 characters in length. The name should unambiguously describe the EOL Configuration.

Ranges	Resistance	Program the eight Resistance settings to define the upper limit of each Band. Eight Bands are available. The resistance range for each Band is from the setting for the previous Band, to the setting of the Band being programmed. e.g. In “Concept3K”, the range for Band 1 is 0 Ohms to 1100 Ohms. For Band 2, 1100 Ohms to 3300 Ohms, etc.
State Mapping	Band States <u>EOL Input States</u> Alarm Mask Orient Fault Range Tamper Low Tamper High Tamper <u>Logical Input States</u> Zone Self-Test Fail Battery Crypto Fail Poll Fail spare Soaking Soak Test Fail Isolate	Select a Zone “State” for each of the Bands that are to be monitored. There are 16 states to choose from, however, normally only one state from the first eight states (Alarm to Tamper) is assigned for a Band.
Miscellaneous Options	Default state debounce time (ms) Alarm state debounce time (ms) Alarm Restore state debounce time (ms)	Minimum time that the Zone Input must remain in an EOL state to process a change. Optional minimum time that the Zone Input must remain in an Alarm EOL state to process a change. Optional minimum time that the Zone Input must <u>not</u> be in the Alarm EOL state to process a change. Note that these options do not apply to legacy Concept Modules.

Access Control

Entity Types and Groups

Entity/Feature	Option	Description
Entity Types	Door Types Qualified Door Types Lift Types Qualified Lift Types Lift Groups	Edit the names, options and permissions of Access Control Entity Types and Groups. Types & Groups simplify the programming of other entities such as Doors and Lifts by providing pre-programmed entities that define operations.

<u>DOOR TYPES</u>		Door Types provide a simple method of defining how Doors of the same type will operate. Door Types are used to define the operation of Doors where the operation is not required to change due to the status of other entities such as Time Periods. IMPORTANT NOTE: If the operation of certain types of Doors is required to change depending on time/date and/or the status of other entities, then “Qualified Door Types” need to be used. (MENU, 2, 4, 5) e.g. If the credential requirements are “Card Only” to enter and REX button to exit during normal business hours, but “Card & PIN” to enter and “Card Only” to exit at other times. A Qualified Door Type consists of one or more Door Types, each paired with a Qualifying entity such as a Time Period or an Area, etc.
Find/Create Door Type.		Select the Door Type you wish to edit.
Name		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Entry Options	User Credential Mode for Entry None Card Only PIN Only Card OR PIN Card AND PIN	Select the User Credential requirement for Entry. None Card must be used. PIN Code must be used. Card or PIN code may be used. User’s Card must be followed by the User’s PIN Code.
	Dual User.	Dual User requirement for entry.

	Anti-Passback Mode for Entry. None Soft Hard Harder Timed	Select the Anti-Passback mode for entry. No Anti-Passback. The Area the User is about to enter is checked against the User's current location. If these Areas are the same, access is still granted, but an Anti-passback violation is logged to Review. The Area the User is about to enter is checked against the User's current location. If these Areas are the same, access is denied and an Anti-passback violation is logged to Review. The Area the User is about to enter, <u>and</u> the Area the Reader is located in, are both checked against the User's current location. If the entry Area is the same or the Reader Area is <u>not</u> the same, access is denied and an Anti-passback violation is logged to Review. Same as Hard Anti-passback, except that Amnesty is automatically applied when the Anti-Passback time for that User expires. For "Hard" and "Harder" Anti-passback, amnesty can be provided for an individual User via the "Set Area User is in" (Uarea) Action.
	Button Mode for Entry. None Enable Deadlock	Defines Entry button operation. Entry button is Disabled Entry button is Enabled Entry button is Enabled, but only while the Area that the button is located in is Off (Disarmed) i.e. The Area on the same side of the Door.
	Entry Area Disarm Options. Disarm Door Entry Area Disarm User Area	Defines Area Disarm operations on entry. Door Area OFF on entry. User Area off on entry.
	Zone Isolate Mode for Entry None Isolate 1 Isolate 2	NOT YET IMPLEMENTED. No Zone Isolation The Zone assigned to the User in Single-Zone mode will be isolated. The Zones assigned to the User in 2-Zone mode will be isolated.
Exit Options	User Credential Mode for Exit None Card Only PIN Only Card OR PIN Card AND PIN	Select the User Credential requirement for Exit. None Card must be used. PIN Code must be used. Card or PIN code may be used. User's Card must be followed by the User's PIN Code.
	Dual User.	Dual User requirement for exit.

	Anti-Passback Mode for Exit. None Soft Hard Harder Timed	Select the Anti-Passback mode for exit. No Anti-Passback. The Area the User is about to enter is checked against the User's current location. If these Areas are the same, access is still granted, but an Anti-passback violation is logged to Review. The Area the User is about to enter is checked against the User's current location. If these Areas are the same, access is denied and an Anti-passback violation is logged to Review. The Area the User is about to enter, <u>and</u> the Area the Reader is located in, are both checked against the User's current location. If the entry Area is the same or the Reader Area is <u>not</u> the same, access is denied and an Anti-passback violation is logged to Review. Same as Hard Anti-passback, except that Amnesty is automatically applied when the Anti-Passback time for that User expires. For "Hard" and "Harder" Anti-passback, amnesty can be provided for an individual User via the "Set Area User is in" (Uarea) Action.
	Button Mode for Exit. None Enable Deadlock	Defines Exit button operation. Exit button is Disabled Exit button is Enabled Exit button is Enabled, but only while the Area that the button is located in is Off (Disarmed) i.e. The Area on the same side of the Door.
	Exit Area Disarm Options. Disarm Door Entry Area Disarm User Area	Defines Area Disarm operations on exit. Door Area OFF on exit. User Area off on exit.
	Zone Isolate Mode for Exit None Isolate 1 Isolate 2	NOT YET IMPLEMENTED. No Zone Isolation The Zone assigned to the User in Single-Zone mode will be De-isolated. The Zones assigned to the User in 2-Zone mode will be De-isolated.

<u>QUALIFIED DOOR TYPES</u>		Qualified Door Types provide a simple method of defining how Doors of the same type will operate, and allow for circumstances where the operation of certain types of Doors is required to change depending on time/date and/or the status of other entities. e.g. If the credential requirements are “Card Only” to enter and REX button to exit during normal business hours, but “Card & PIN” to enter and “Card Only” to exit at other times. A Qualified Door Type consists of a list of one or more Door Types, each paired with a Qualifying entity such as a Time Period or an Area, etc. If a Qualified Door Type is assigned to a Door, then on any access attempt, the Door operation is determined by the first Door Type in the list that is currently valid. If more than one Door Type is used in a Qualified Door Type, and there is a possibility that more than one Door Type may be valid at the same time, it is important to consider the order in which the Door Types are assigned. i.e. The Door Types in the Qualified Door Type are prioritised from Q1 to Q8. IMPORTANT NOTE: If the Door operations are <u>not</u> required to change due to the status of other entities then “Door Types” should be used. (MENU, 2, 4, 2)
Find/Create Qualified Door Type.		Select the Qualified Door Type you wish to edit.
Name.		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Door Types	Door Types What When	Program or Edit the first Door Type for this Qualified Door Type. The “What” <u>must</u> be a Door Type that defines how the Door is to operate. The “When” will be an entity that will define when the Door is to operate in this way. e.g. Typically a Time Period or an Area status. Up to 8 Door Types can be assigned to a Qualified Door Type.

<u>LIFT TYPES</u>	See the “Integriti Lift Interfacing” document for a full description of Integriti Lift Access Control.	Lift Types provide a simple method of defining how Lifts of the same type will operate. Lift Types are used to define the operation of Lifts where the operation is not required to change due to the status of other entities such as Time Periods. IMPORTANT NOTE: If the operation of certain types of Lifts is required to change depending on time/date and/or the status of other entities, then “Qualified Lift Types” need to be used. (MENU, 2, 4, 5) e.g. If the credential requirements are “Card Only” to enter and REX button to exit during normal business hours, but “Card & PIN” to enter and “Card Only” to exit at other times. A Qualified Lift Type consists of one or more Lift Types, each paired with a Qualifying entity such as a Time Period or an Area, etc.
Find/Create Lift Type.		Select the Lift Type you wish to edit.
Name		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Entry Options	User Credential Mode for Entry	Select the User Credential requirement for Entry.
	None Card Only PIN Only Card OR PIN Card AND PIN	None Card must be used. PIN Code must be used. Card or PIN code may be used. User’s Card must be followed by the User’s PIN Code.
	Dual User.	Dual User requirement for entry.
	Anti-Passback Mode for Entry.	Select the Anti-Passback mode for entry.
	None Soft Hard Harder Timed	No Anti-Passback. The Area the User is about to enter is checked against the User’s current location. If these Areas are the same, access is still granted, but an Anti-passback violation is logged to Review. The Area the User is about to enter is checked against the User’s current location. If these Areas are the same, access is denied and an Anti-passback violation is logged to Review. The Area the User is about to enter, <u>and</u> the Area the Reader is located in, are both checked against the User’s current location. If the entry Area is the same or the Reader Area is <u>not</u> the same, access is denied and an Anti-passback violation is logged to Review. Same as Hard Anti-passback, except that Amnesty is automatically applied when the Anti-Passback time for that User expires. For “Hard” and “Harder” Anti-passback, amnesty can be provided for an individual User via the “Set Area User is in” (Uarea) Action.

	Button Mode for Entry. None Enabled Deadlock	Defines Entry button operation. Entry button is Disabled Entry button is Enabled Entry button is Enabled, but only while the Area that the button is located in is Off (Disarmed) i.e. The Area on the same side of the Door.
	Entry Area Disarm Options. Disarm Door Entry Area Disarm User Area	Defines Area Disarm operations on entry. Door Area OFF on entry. User Area off on entry.
	Zone Isolate Mode for Entry None Isolate 1 Isolate 2	NOT YET IMPLEMENTED. No Zone Isolation The Zone assigned to the User in Single-Zone mode will be isolated. The Zones assigned to the User in 2-Zone mode will be isolated.
Exit Options NOT YET IMPLEMENTED.	User Credential Mode for Exit None Card Only PIN Only Card OR PIN Card AND PIN	Select the User Credential requirement for Exit. None Card must be used. PIN Code must be used. Card or PIN code may be used. User's Card must be followed by the User's PIN Code.
	Dual User.	Dual User requirement for exit.
	Anti-Passback Mode for Exit. None Soft Hard Harder Timed	Select the Anti-Passback mode for exit. No Anti-Passback. The Area the User is about to enter is checked against the User's current location. If these Areas are the same, access is still granted, but an Anti-passback violation is logged to Review. The Area the User is about to enter is checked against the User's current location. If these Areas are the same, access is denied and an Anti-passback violation is logged to Review. The Area the User is about to enter, <u>and</u> the Area the Reader is located in, are both checked against the User's current location. If the entry Area is the same or the Reader Area is <u>not</u> the same, access is denied and an Anti-passback violation is logged to Review. Same as Hard Anti-passback, except that Amnesty is automatically applied when the Anti-Passback time for that User expires. For "Hard" and "Harder" Anti-passback, amnesty can be provided for an individual User via the "Set Area User is in" (Uarea) Action.
	Button Mode for Exit. None Enable Deadlock	Defines Exit button operation. Exit button is Disabled Exit button is Enabled Exit button is Enabled, but only while the Area that the button is located in is Off (Disarmed) i.e. The Area on the same side of the Door.

	Exit Area Disarm Options. Disarm Door Entry Area Disarm User Area	Defines Area Disarm operations on exit. Door Area OFF on exit. User Area off on exit.
	Zone Isolate Mode for Exit None Isolate 1 Isolate 2	NOT YET IMPLEMENTED. No Zone Isolation The Zone assigned to the User in Single-Zone mode will be De-isolated. The Zones assigned to the User in 2-Zone mode will be De-isolated.

<u>QUALIFIED LIFT TYPES</u>	See the “Integriti Lift Interfacing” document for a full description of Integriti Lift Access Control.	Qualified Lift Types provide a simple method of defining how Lifts of the same type will operate, and allow for circumstances where the operation of certain types of Lifts is required to change depending on time/date and/or the status of other entities. e.g. If the credential requirements are “Card Only” to enter and REX button to exit during normal business hours, but “Card & PIN” to enter and “Card Only” to exit at other times. A Qualified Lift Type consists of a list of one or more Lift Types, each paired with a Qualifying entity such as a Time Period or an Area, etc. If a Qualified Lift Type is assigned to a Lift, then on any access attempt, the Lift operation is determined by the first Lift Type in the list that is currently valid. If more than one Lift Type is used in a Qualified Lift Type, and there is a possibility that more than one Lift Type may be valid at the same time, it is important to consider the order in which the Lift Types are assigned. i.e. The Lift Types in the Qualified Lift Type are prioritised from Q1 to Q8. IMPORTANT NOTE: If the Lift operations are <u>not</u> required to change due to the status of other entities then “Lift Types” should be used. (MENU, 2, 4, 2)
Find/Create Qualified Lift Type.		Select the Qualified Lift Type you wish to edit.
Name.		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Lift Types	Lift Types What When	Program or Edit the first Lift Type for this Qualified Lift Type. The “What” <u>must</u> be a Lift Type that defines how the Lift is to operate. The “When” will be an entity that will define when the Lift is to operate in this way. e.g. Typically a Time Period or an Area status. Up to 8 Lift Types can be assigned to a Qualified Lift Type.

Lift Group Programming

See the “Integriti Lift Interfacing” document for a full description of Integriti Lift Access Control.

Entity/Feature	Option	Description
Find Lift Group		Select Lift Group to program. Lift Groups are required when a high-level interface (EMS Comms Task format) is used. Not required for low-level interface.
Lift Group Name		Program a text name of up to 32 characters in length. The first screen is used to program the first 16 characters and the second screen is used to program the remaining 16 characters if required.
EMS Floor Mapping		Assign each Floor ID of the EMS to the required Integriti Controller Floor record. For each Floor: • Add the Integriti Floor to be mapped. • Enter an EMS Floor number. • If the Floor record is for a Rear Door, then enable the “Rear Door” option.
Settings	EMS Rise	Enter the Rise number to send to an EMS system for Lifts in this Group. The number must be 1 or greater.
	EMS Group	Enter the Group number to send to an EMS system for Lifts in this Group. The number must be 1 or greater.
	Number of Floors	Enter the number of Floors in this Group. If left at 0, the largest EMS Floor number will be used.

Access Control Entities

Card Formats

Entity/Feature	Option	Description
Card Format		Select a Card format to program. Integriti provides an extensive range of pre-programmed Card Formats that will cater for the vast majority of applications. An additional Card format would only need to be programmed to cater for a less common proprietary format or a newly developed format not already provided in the Integriti Card Formats. Please report additional format requirements to Inner Range Support for inclusion in future updates.

Options	Card Type	Each card format has a card type defined. The Card Type will tell the reader how to operate, including whether to expect Magnetic Stripe or Wiegand card data, whether it needs to convert the raw data to site code, card number and issues number, or if it needs to hash or decrypt the card data (e.g. Credit Card or IR Secure40). The additional programming fields displayed will vary depending on the Card Type chosen in this option. Select the Card Type to be used in this format.
	None	No Card Type selected.
	Wiegand Raw Data	For direct entry Wiegand cards of any length. (If migrating the card database from a Concept 3000/4000 system you may wish to use the "Legacy: C3k Raw Data" Type.)
	Wiegand Site Code	Allows user credentials to be entered as site code and card number providing the format is known.
	IR Secure 40	Decrypts an IR Secure 40 card and matches it on Site Code and Card Number.
	Mag Swipe Raw Data	Reads up to the first 22 characters of a mag card, until it gets an end or separator sentinel character.
	IR Mag Swipe	Decrypts a Concept Secure Magnetic card and returns its site code, card number and issue number.
	Mag Swipe Site Code	Reads magnetic cards in character mode. Allows user definable site code parameters to be programmed, except lengths and offsets are specified in characters instead of bits.
	Hashed Credit Card	Reads the first 22 characters from a mag card and generates a 5 byte hash from this using the same algorithm as the Concept "Credit Card" format.
	Wiegand Site (Complex)	Allows for Site Code formats unknown to Inner Range. This is the recommended format when only one card format is used throughout the system.
	40 Bit Mag Raw Data	This magnetic swipe card format read the first 10 characters (40 bits) from a mag card, nibble swapping each byte (ie: swapping each character pair). This allows for compatibility in migrations where Concept Mag Direct was used.
	Mag Swipe Site Code (bits)	This format makes the reader return the binary data from the card instead of characters. This supports non "ISO Track 2" cards where the site code and card number info is stored as binary data instead of characters.
	Legacy: C3k Raw Data	Reads the Wiegand card data and removes the start bit. This helps migrations from Concept direct entry Wiegand systems where the start bit was not used (i.e. Most C3k/C4k Wiegand Direct Entry installations).

Site Code Parameters	Total Bits Site Code Offset Site Code Length Card Number Offset Card Number Length Issue Number Offset Issue Number Length	If a Site Code Card Type is selected above, this option allows the Card data parameters to be defined. The total number of bits present in the Card's data. The number of bits in the string prior to the Site Code data. The number of bits in the Site Code data. The number of bits in the string prior to the Card Number data. The number of bits in the Card Number data. The number of bits in the string prior to the Issue Number data. (If used) The number of bits in the Issue Number data. (If used) e.g. If the card data string is 38 bits where Bit 1 is Parity, Bits 2 to 17 are Site Code Data, Bits 18 to 37 are Card Number and Bit 38 is Parity, the settings would be programmed as follows: Total Bits: 38 Site Code Offset: 1 Site Code Length: 16 Card Number Offset: 17 Card Number Length: 20 Issue Number Offset: 0 Issue Number Length: 0
	Secure 40 Scheme Type Standard Registered Site Enterprise	If the Inner Range Secure 40 Card Type is selected above, choose the IR Secure 40 scheme that will apply to this Card Format. The Scheme is shown on the label affixed to the box that the cards were supplied in. Registered Site Cards will also have the text "RS[nn]" printed on them, where nn is the production batch number. Standard. Over 32,000 Site Codes and Card Numbers up to 65,535. Registered Site. Unique Client Site Codes factory registered and Card Numbers up to 65,535. Enterprise. Unique Client Site Codes factory registered and Card Numbers up to 1,048,575.

Card Programming	Wiegand Card Type	For all Card Types in a Wiegand format, an option is provided to select a Wiegand Card Type. This can be N Bit meaning that any bit length is allowed or it can be set to a particular bit length. N Bit will always return all the bits read. For fixed bit lengths, the behaviour varies between legacy Concept Modules and Integrity Modules. Legacy Modules: For cards equal to or longer than the bit length, it will return the first n bits, as if the card read were n bits long. If the card is shorter than the bit length, it is ignored. Integrity Modules: If the card is not equal to the bit length, it is ignored completely. If a Wiegand Card Type is selected above, select the Wiegand Card Type required.
	26 Bit 27 Bit 30 Bit 32 Bit 34 Bit 35 Bit 36 Bit 37 Bit N Bit Secure 40	26 Bits 27 Bits 30 Bits 32 Bits 34 Bits 35 Bits 36 Bits 37 Bits Any bit length is allowed. Inner Range Secure 40 Bits

Door Programming

Entity/Feature	Option	Description
Door		Select a Door to program.
Door Name		Program a text name of up to 32 characters in length. The Door Name may include the location and/or type of the Door.
Module		Select the Module that the Door Reader and hardware are connected to.
Relay	No Lock Lock 1 Lock 2 Lock 3 Lock 4 Lock 5 Lock 6 Lock 7 Lock 8	Select the Lock Relay to be used for this Door.

Door Type	Default Door Types: Entry Door Exit Door Internal (RIRO) Door Card+PIN Entry Door Card+PIN Exit Door Card+PIN Internal (RIRO) Door	Select the Door Type or Qualified Door Type for use with this Door. The selected Door Type or Qualified Door Type will determine how this particular door will function. Door Types and Qualified Door Types are programmed separately The 6 default Door Types shown opposite cover common Door Access Control requirements. Additional Door Types or Qualified Door Types may be programmed. If a Qualified Door Type is assigned, then on any access attempt, the Door operation is determined by the first Door Type in the list that is currently valid.
Outside Settings	Reader None Reader 1 Reader 2 ... Reader 16	Select the Module Reader Port to be used for the Outside Reader. From 1 to 16 Readers may be available depending on the Module Type.
	PIN Device. None Motorola HID Reader MR Access Model Reader 26 Bit Wiegand Keypad IR Weatherproof Terminal 26Bit Wiegand Keypad Forced	If the Outside Reader is a PIN code device, select PIN device type. No PIN device. Motorola/Indala ARK-501 HID 5355 or iClass with 4 Bit Burst PIN output format. MR Access Magnetic Swipe & PIN code Reader 26 Bit Wiegand Keypad. Inner Range Weatherproof Terminal. If enabled, any 26 bit Wiegand data received from this Reader will be processed as a PIN Code regardless of the Site Code. Cards will not be able to be used at this Reader. If disabled, only 26 bit Wiegand data with Site Code 255 (FF) will be processed as a PIN Code and any other Site Code will be processed as a Card.
	Area	Select the Area to be associated with the Outside of this Door. (The "Exit" Area) Required for operations and functions that use the Area status or data such as Reader Arming/Disarming, Anti-passback, User Counting, etc.
	Arm Mode None Button 3 Badge Area Empty	Select the Area Arming Mode for this Reader if required.
Inside Settings	Reader	Select the Module Reader Port to be used for the Inside Reader. Options as above.

	PIN Device	If the Inside Reader is a PIN code device, select PIN device type. Options as above.
	Area	Select the Area to be associated with the Inside of this Door. (The “Entry” Area) Required for operations and functions that use the Area status or data such as Reader Arming/Disarming, Anti-passback, User Counting, etc.
	Arm Mode	Select the Area Arming Mode for this Reader if required. Options as above.
	ADVANCED	
Door Configuration	Door Type	See above.
	Inside Area	See above.
	Outside Area	See above.
	Door State Follows Area State None Inside Area Outside Area Either Area Both Areas	Select if the Door state is to be controlled by the Inside and/or Outside Area. i.e. Door will Unlock if Area Disarmed, and will Lock if Area is Armed. Door state does not follow Area State. Door state follows Inside Area State. Door state follows Outside Area State. Door state is Locked when either the Inside <u>or</u> Outside Area is Armed, and will Unlock when both Areas are Disarmed. Door state is Locked when the Inside <u>and</u> Outside Areas are both armed, and will Unlock when either Area is Disarmed.
	Physical Type Normal Roller (Up – Down) Roller (Toggle)	Select the physical type of the Door. Normal Door. A Roller Door that requires separate outputs from the controller for Up and Down control. A Roller Door that requires a single timed output from the controller on which each activation toggles between Up and Down. <i>See “Roller Doors” following the Door programming for details.</i>
	Inhibit Input	If a Roller Door type is selected above, an Inhibit Input may be programmed. The Inhibit Input is installed to detect something blocking the physical path of the Roller Door. e.g. A PE (Photo Electric) beam installed immediately inside the Roller Door to detect the presence of a pedestrian or vehicle under the raised Door.
Advanced Door Configuration	Lock Auxiliary	Hardware Auxiliary address for Door lock. Programmed only when the door does not use the predefined local lock auxiliary of the Reader/Terminal.

	Door Unlock Time	Determines how long the door lock auxiliary remains On when the Door is accessed. Programmed in Hours, Minutes and Seconds up to a maximum of 18 Hrs, 12 Mins and 15 Seconds.
	Disabled Unlock Time	Determines how long the door lock auxiliary remains On when the Door is accessed by Users that have the “disabled” option enabled. Programmed in Hours, Minutes and Seconds up to a maximum of 18 Hrs, 12 Mins and 15 Seconds.
	Door Open Too Long (DOTL) Time.	Determine how long a door may remain open until a DOTL warning or alarm is generated. If the Door remains open longer than this time, then: - If a DOTL Warning Time is <u>not</u> programmed, the relevant DOTL (Door Held) System Input on the Module will go into alarm. - If a DOTL Warning Time <u>is</u> programmed (see below), the relevant local DOTL Warning output on the Module will be turned on for the Warning Time. If the Door continues to remain open for longer than the warning time, the relevant DOTL (Door Held) System Input on the Module will go into alarm. Programmed in Hours, Minutes and Seconds up to a maximum of 18 Hrs, 12 Mins and 15 Seconds.
	Door Open Too Long (DOTL) Warning Time.	Determines the DOTL Warning timer period. <i>See “Door Open Too Long (DOTL) Time” above for details.</i>
	Interlock Group	Defining an Interlock Group restricts access through this door based on the state of entities in the Interlock Group programming. e.g. Access to a Door into an airlock can be disabled while any other Door into the same airlock is Unlocked and/or Open.
Anti-Passback	Entry Area Anti-Passback Minutes	Defines the Timed Anti-Passback period for an anti-passback violation on the Entry Area. <i>See “Anti-Passback Mode” in Door Types programming for details.</i>
	Exit Area Anti-Passback Minutes	Defines the Timed Anti-Passback period for an anti-passback violation on the Exit Area. <i>See “Anti-Passback Mode” in Door Types programming for details.</i>

Options	Tenancy Area Counting.	If enabled: On a successful Door access control operation, and the direction is leaving, then the number of Users in the User's Tenancy Area will be decremented. Any resultant Area User Count Action will also be invoked. If direction is entering then the number of Users in the User's Tenancy Area will be incremented. Any resultant Area User Count Action will also be invoked. i.e. The User Count will be updated in the User's Tenancy Area instead of the Door Inside Area. Notes: 1. The User's Tenancy Area must be defined. 2. The Dual User option should not be used with Tenancy Area Counting. If not enabled: On a successful Door access control operation, the number of Users in the Door Area that you are leaving will be decremented (twice if Dual User) and the number of Users in the Door Area that you are entering will be incremented (twice if Dual User). Any resultant Area User Count Action will also be invoked. i.e. User counting is performed on the Area/s assigned to the Door.
Debounce	Forced Door Debounce.	This option will shunt the reed/tongue for this time after the door is unlocked. This is to stop the panel accidentally relocking the door due to bounce as it is opened. While the door is unlocked if the panel senses the door open, it will wait for it to close again. When it closes the panel will automatically relock the door, even if the lock timer hasn't expired.
Inside Area	Find iArea Name^ None	Select the Area that is on the inside of the Door. Inside Area is defined when security arming and user control features are required.
Outside Area	Find oArea Name^ None	Select the Area that is on the outside of the Door. Outside Area is defined when security arming and user control features are required. Normally left set to "None" if the Door is a perimeter Door. i.e. If exiting through the Door takes you out of all areas being protected by the system.
Behaviour	Free Access	If the Door is required to be in Free Access under certain conditions, select the entity that will define the Free Access conditions. e.g. A Time Period or Schedule.
Miscellaneous Options	Offline Behaviour	Select an "Offline Permission" for this Door to define how it will operate if the host Module is offline.
Card Format		Select the Card Format to be used for access control operations at this Door.

Roller Doors

Options are provided in Door programming to define a physical Door type of "Roller (Up – Down)" or "Roller (Toggle)".
Roller (Up – Down) is a Roller Door that requires separate outputs from the controller for Up and Down control.

Roller (Toggle) is a Roller Door that requires a single timed output from the controller on which each activation toggles between Up and Down.

To implement Roller Door control, a Reed Switch is installed (door reed input) that seals when the door is fully closed, and an optional reed switch is installed (tongue sense input) that seals when the door is fully open.

The complete list of Input and Output states used for Roller Doors is as follows:

Door reed sealed	Roller door fully down (locked)
Door reed in alarm	Roller door not fully down
Tongue reed sealed	Roller door fully up (locked) (tongue input must be enabled)
Tongue reed in alarm	Roller door not fully up (tongue input must be enabled)
Door Lock output	Roller up output (or toggle output for toggle type doors)
Door DOTL output	Roller down output (only for up/down type doors)
Door Tamper Input	Alarms when a roller door fault occurs, seals when tries again
Door DOTL Input	Alarms at start of down warning, seals at end of down warning (Program an action to the Door DOTL Input to annunciate a door down warning)
Door Forced Input	Alarms if the door is currently fully opening, and is being prevented from closing by the Door inhibit input (see below)
Door Inhibit Input	Pauses a door going down via an input (e.g. safety beam) When input re-seals door continues down Doesn't work for toggle mode doors

The following Door and Reader Module programming options are required to implement Roller Door control:

- Set the Physical Door Type option to Up/Down roller door or Toggle roller door.
- Set the "Door Unlock Time" to the maximum time it takes to open the roller door, or if tongue sense is not enabled, the time that the roller door requires to reach its desired open position.
- Set the "Extended Unlock Time" to the maximum time it takes to close the roller door.
- Set the "Door Open Too Long Time" to the maximum time it takes the roller door to signal it is now opening/closing via the reed or tongue inputs.
- Set the "Warn Time" to the time that the DOTL input will remain in alarm as a warning prior to the roller door closing (going down warning)
- Set "Force Debounce" time to set the time the toggle relay turns on for in toggle mode (Also sets the gap between toggles)
- Select the "Inhibit Input" if being used.
- The Reader Module "Enable Tongue Input" option is set for the appropriate Door if a reed is installed to indicate the roller door is fully open (connected to the tongue sense input).

The roller state machine is designed to try and get the roller door either open (if the door is unlocked) or closed (if the door is locked).

The roller state machine does not alter the lock status of the door - it simply tries to manipulate the roller door to get it into the correct state.

If the roller doors cannot be got into the correct state to match the lock status of the door, then a "Fault" state is assumed and no more effort is made to get the roller door to match the door lock status until another lock(or relock) or unlock (or re-unlock) attempt is made.

Whilst in the "Fault" state, the door tamper input is in the alarm condition indicating a problem. If a door is currently up and is being prevented from closing because of the inhibit input, then the door forced input will be in alarm.

All attempts to close (lock) a roller door are preceded by a "Down Warning" state. This state puts the door DOTL input into alarm which can be used to warn personnel that the door is about to close. At the end of the warning time the door attempts to close. Once the door direction down is established, if the inhibit input is sensed in alarm then the door will revert to going up. When a card is presented or REX/REN button pushed and the door is a roller door, then the current lock state of the door is toggled. i.e. Lock to unlock or unlock to lock.

A Motor overload output can be wired to tamper either reed or tongue input to immediately cause the fault input state.

Note on Inhibit Input and Roller Door toggle mode: In toggle mode, the lock output pulses to reverse the direction of the door, i.e. going up or going down. The roller state machine attempts to deduce the correct direction the door is travelling, however,

it is possible under abnormal circumstances that the door direction is not ascertained correctly. This can result in the inhibit input not successfully stopping a closing door. When using toggle mode, another means must also be used to sense door obstructions.

Note on tongue sense: If tongue sense is disabled, then the state machine uses the “Door Unlock Time” to determine when the door is considered to be fully open from fully closed. Note that subsequent locks and unlocks could result in the door going higher than desired.

It is not recommended to have tongue sense disabled in toggle mode because when the door is in the open state, there is no way to see if the toggle state is correct by monitoring for an alarm on the tongue reed switch (door fully open).

Lift Car Programming

See the “Integriti Lift Interfacing” document for a full description of Integriti Lift Access Control.

Entity/Feature	Option	Description
Lift Car		Select a Lift Car to program.
Name		Program a text name of up to 32 characters in length. The Lift Car Name may include the location and/or type of the Lift.
Restricted Floors		If the Lift Car does not service all Floors, permissions may be programmed to define one or more Floors or Floor Lists that are serviced (by selecting “Allow”) and/or are not serviced (by selecting “Deny”) by this Lift Car and when these restrictions apply. Up to ?? Restricted Floor Permissions may be assigned.
Lift Configuration	Lift Mode None Low Level (No Button Feedback) Low Level (Button Feedback) High Level / EMS	Select the Interface Mode used for this Lift Car. None Low Level Lift interface with no Button Feedback Low Level Lift interface with Button Feedback High Level Lift interface via Serial or Ethernet communications.
	Lift Type	Select the Lift Type or Qualified Lift Type for use with this Lift Car. The selected Lift Type or Qualified Lift Type will determine how this particular Lift will function. Lift Types and Qualified Lift Types are programmed separately. There are no default Lift Types. If a Qualified Lift Type is assigned, then on any access attempt, the Lift operation is determined by the first Lift Type in the list that is currently valid.

	Hardware Control Point	If a Low Level interface is in use, select the first Auxiliary that will be used for Floor button enables. The Floor Button enable Auxiliaries will be a continuous sequence of Auxiliaries starting at this Auxiliary and continuing up to the number of Floors defined in “Lift Floors” below. After the last Auxiliary on the Module, you move to the next Auxiliary on the next sequential module (E01:32 to E02:X01)
Options	Add Floors Use 2 nd Enables Destination Panel	Set to Yes IF you require additional Floor buttons to immediately be enabled when another User presents their Card to the Reader while the previous User’s buttons are still enabled. Set to Yes if you require the previous User’s enabled buttons to be cancelled when another User presents their Card to the Reader. This Lift Car is logically a Destination Panel (Only relevant to some High Level Lift interfaces)
General	Button On Time	Program the Button time in Hours, Minutes and Seconds.
	Disabled Button On Time	Program the Button time for Disabled Users in Hours, Minutes and Seconds.
	Button Enable Hold Time	If Button Feedback is in use, program the Button Enable Hold Time in Days, Hours, Minutes and Seconds. This option defines the time that the Floor buttons remain enabled after button feedback is received.
Miscellaneous Options	Floor Auxiliary	Not yet implemented.
	Error Auxiliary	Select an Auxiliary to be used to indicate an error in the Lift access control process.
	Lift Group	If High Level interface is in use, select a Lift Group to define the EMS parameters for this Lift Car. Lift Groups are programmed separately.
	EMS Lift Number	If High Level interface is in use, program an EMS Lift Number to identify this Lift Car to the EMS.
	Destination Panel ID	If High Level interface is in use, and this Lift Car is a logical Destination Panel, program the Destination Panel ID for this Lift Car.
	Lift Floors	Define the Floors to be serviced by this Lift Car.

Floor Programming

See the “Integriti Lift Interfacing” document for a full description of Integriti Lift Access Control.

Entity/Feature	Option	Description
Floor		Select a Floor to program.

Name		Program a text name of up to 32 characters in length. The Floor Name may include the location of the Floor.
Associated Area		Select an optional Area to be associated with this Floor if required.

Automation and Logic Functions

Entity/Feature	Option	Description
Named Actions		Program/Edit Named Actions.
Macros		
Air-conditioning		
Comparisons		Program/Edit Comparisons.
Calibrations		
Compound Entities		Allows multiple entities to be combined logically for use as a Qualifier in Permissions.
General Variables		
General Timers		

Named Actions

Entity/Feature	Option	Description
Named Action		Select the Named Action to program or edit. Named Actions allow Users to perform predefined actions from a Terminal. Options are also provided to allow the Named Action to be controlled by another Entity.
Name		Program a text name of up to 32 characters in length.
Action		Select the Entity Type to be controlled by this action. Once an Entity Type is selected, additional fields are displayed to program the Action details. <i>See Action Programming in “Generic Programming Operations” for more details.</i>
Optional Trigger		Select an Entity that will trigger this Named (Predefined) Action. e.g. An Input, Time Period, Auxiliary, Door, etc.
Interface Style	None On / Off Open / Close Air Conditioning Auxiliary Control Trigger	Select the User Interface style to be used when this Named (Predefined) Action is operated manually via a Terminal. No style On / Off Open / Close Air-conditioning Auxiliary Trigger

	Sense Entity 1. LCD Terminal Graphic Terminal	Select the primary Entity to display the state of this Named Action. Currently an LCD Terminal or Graphic Terminal may be chosen.
	Sense Entity 2 to Sense 4.	Select up to 3 additional Entities to display the state of this Named Action.
	Allow Logged off access.	The Named Action can be controlled from a Terminal without the User logging on.
Action Groups		This option allows Named Actions to be grouped together in up to 16 Action Groups for the purpose of defining which Users and Entities are allowed to control which Actions. The Named Actions allowed to be controlled from an LCD or Graphic Terminal, or by particular Users or Types of Users are defined via similar screens in Menu Group programming. The Menu Group can then be assigned to an LCD Terminal or Graphic Terminal, a User and/or Permission Group. Select which of the 16 Action Groups this Named Action will belong to.

Macros

Entity/Feature	Option	Description
Macro		Select the Macro to program or edit.
Name		Program a text name of up to 32 characters in length. The name may include the purpose and/or some details of the Macro.
Type	Do an Action Do an Action when the Expression Changes Goto <label> If Pause for Time Define a Label Set Entity to Expression Wait for Condition Execute Modified Action End Current Macro	Select the Type of Macro to program.
Action		If the Macro Type is: - Do an Action - Do an Action when Expression changes - Execute Modified Action... Select the Entity Type to be controlled by this action. Once an Entity Type is selected, additional fields are displayed to program the Action details. <i>See Action Programming in “Generic Programming Operations” for more details.</i>

Expression		If the Macro Type is: - Do an Action when Expression changes - Goto <label> if... - Pause for Time... - Set Entity to Expression - Wait for Condition Program the Expression. Expressions can evaluate to true or false, or to a number, depending on the context in which they are used.
Label		If the Macro Type is: - Goto <label> if... - Define a Label Program the Label.
Entity to Set		If the Macro Type is: - Set Entity to Expression Select the Entity. Nearly all entities can return a numerical value. For instance an Input can hold a count value. This statement changes the entities value to the value returned by the expression, which could be a constant, another entity, or a maths formula involving any of these. This is primarily how GVars get set to a value.
Entity 1 Entity 2 Entity 3 Entity 4		If the Macro Type is: - Execute Modified Action... Select up to 4 Entities to define the numeric parameters for the action. The numeric value returned by the first entity will set the first numeric parameter for the action, the second entity the second parameter. So if the action were “control an auxiliary” and the first entity is a count Input, the on time of the aux action would be determined by the count value in the Input.
Comment		If the Macro Type is: - Do an Action - Do an Action when Expression changes - Goto <label> if... - Pause for Time... - Define a Label - Set Entity to Expression - Wait for Condition - Execute Modified Action... - End Current Macro You may enter a comment in this field. Just like comments in programming language, allows the programmer to document the intended functionality of each line.
Statements		

Air-conditioning

Entity/Feature	Option	Description
Air-conditioner		Select the Air-conditioning Unit to program or edit.
Name		Program a text name of up to 32 characters in length.
Temperature Sensors		Select the Inputs to be used for Temperature Sensing. Up to 8 Inputs may be selected, one for each Air-conditioning Zone.
Damper Auxiliaries		Select the Auxiliaries to be used to control the Zone Dampers. Up to 8 Auxiliaries may be selected, one for each Air-conditioning Zone.
Compressor Auxiliary		Select the Auxiliary to be used to control the Compressor.
Reverse Cycle Auxiliary		Select the Auxiliary to be used to control Reverse Cycle On/Off.
Fan Auxiliary		Select the Auxiliary to be used to control the Fan.
Fresh Air Damper Auxiliary		Select the Auxiliary to be used to control the Fresh Air Damper.
Bypass Damper Auxiliary		Select the Auxiliary to be used to control the Bypass Damper.
Minimum Compressor ON Time.		Determines the Minimum Compressor On Time. Enter a value in Hours, Minutes and Seconds. A Value of up to 1 Hr, 49 Min and 13 Seconds can be entered.
Minimum Compressor OFF Time.		Determines the Minimum Compressor Off Time. Enter a value in Hours, Minutes and Seconds. A Value of up to 1 Hr, 49 Min and 13 Seconds can be entered.
Damper Time		Determines the Damper On Time. Enter a value in Hours, Minutes and Seconds. A Value of up to 1 Hr, 49 Min and 13 Seconds can be entered.
Return Air Zone		Defines the Air-conditioning Zone where the Return Air Damper is located.
Minimum Zones for Bypass		Defines the minimum number of zone dampers that can be open before the compressor bypass damper will be closed. If less than this number of zone dampers are open, the bypass damper output will turn off thus opening the bypass damper to lessen air flow from the fan. If this option is left at 0, the bypass damper will remain closed.

Comparisons

Entity/Feature	Option	Description
Comparison to Edit		Select the Comparison to program or edit. Comparisons provide the ability to trigger actions when certain analogue or count values are reached on an Input.

Comparison Name		Program a text name of up to 32 characters in length.
Input and Thresholds	Input to Monitor	Select an Analogue or Counter type Input to Monitor.
	Threshold 1	Enter the Threshold 1 value. The un-calibrated Analogue or Count value representing the required threshold must be used.
	Threshold 2	Enter the Threshold 2 value.
Inputs to Trigger	Input for Threshold 1	Select an optional Input to Trigger for Threshold 1. The alarm state of the selected Input will be asserted if the monitored Input is above Threshold 1. The alarm state will be de-asserted if the monitored Input is below or equal to Threshold 1. An Input trigger will be required if you wish the event to be reported.
	Input for Threshold 2.	Select an optional Input to Trigger for Threshold 2. The alarm state of the selected Input will be asserted if the monitored Input is above Threshold 2. The alarm state will be de-asserted if the monitored Input is below or equal to Threshold 2. An Input trigger will be required if you wish the event to be reported.
Threshold 1 Action.	Action 1	Select Entity Type for Threshold 1 Action. Once an Entity Type is selected, additional fields are displayed to program the Action details. <i>See Action Programming in “Generic Programming Operations” for more details.</i>
	When Above Threshold 1. None Assert De-assert	Choose what to do for Action1 when Above Threshold 1. No state triggered when above Threshold 1. State Asserted when above Threshold 1. State De-asserted when above Threshold 1.
	When Below Threshold 1. None Assert De-assert	Choose what to do for Action1 when Below Threshold 1. No state triggered when below Threshold 1. State Asserted when below Threshold 1. State De-asserted when below Threshold 1.
Threshold 2 Action.	Action 2	Select Entity Type for Threshold 2 Action. Once an Entity Type is selected, additional fields are displayed to program the Action details. <i>See Action Programming in “Generic Programming Operations” for more details.</i>
	When Above Threshold 2. None Assert De-assert	Choose what to do for Action2 when Above Threshold 2. No state triggered when above Threshold 2. State Asserted when above Threshold 2. State De-asserted when above Threshold 2.

	When Below Threshold 2.	Choose what to do for Action2 when Below Threshold 2.
	None	No state triggered when below Threshold 2.
	Assert	State Asserted when below Threshold 2.
	De-assert	State De-asserted when below Threshold 2.

Compound Entities

Entity/Feature	Option	Description
Compound Entity		Select the Compound Entity to program or edit. Compound Entities enable up to eight different Entities to be logically combined for use as a Qualifier in Permissions. How cool is that?
Name		Program a text name of up to 32 characters in length. The name may include the purpose of the Compound Entity and/or a summary of the entities associated with it.
Define Entities and Relationships		Up to 8 Entities may be assigned to a Compound Entity. For each Entity assigned, an “Invert” option and logical relationship may be defined. The programming options below are repeated for each of the eight Entities.
Entity Selection		Select an Entity to include in this Compound Entity.
Invert Entity	User Door Door List Area Area List Input Auxiliary Time Period Schedule Holiday	Enable this option if you require the logic for this Entity to be Inverted. Normally the different Entity types will be considered Valid in the state shown in the table below. Enable this option if you require the Entity to contribute a Valid condition to the Compound Entity when in the <u>opposite</u> state. ??? Locked and Closed. All Locked and Closed. Armed All Armed Sealed On Valid Valid Valid

Logical Relation	And Or eXclusive OR (XOR)	Select the logical relationship of this Entity to the next Entity. This Entity is ANDed with the following Entity This Entity is ORed with the following Entity XOR logic is applied to these Entities. i.e. The result is Valid if <u>either</u> entity is Valid and Invalid when <u>both</u> Entities are either Valid or Invalid. The logic is applied in the order in which it is entered. The first two Entities take the first Logical Relation (operator). The second Logical Relation is applied to the result of the first two entities and the third entity. The third Logical Relation is applied to the previous result and the fourth entity, etc. Imagine A, B, C, D, and E are entities 1 to 5 respectively and 1, 2, 3 and 4 are Logical Relations 1 to 4 respectively. The expression would be: (((A 1 B) 2 C) 3 D) 4 E).
------------------	---------------------------------	---

General Variables

Entity/Feature	Option	Description
General Variable		Select the General Variable to program or edit. General Variables provide a place to store a value and perhaps do something when that value reaches a certain threshold.
Name		Program a text name of up to 32 characters in length.
Test Value		Program a Test Value. The Variable will be True if the General Variable value is greater than this number.
Calibration		Select a Calibration for this General Variable to define the formatting of the General Variable. Calibrations are programmed separately.

General Timers

Entity/Feature	Option	Description
General Timer		Select the General Variable to program or edit. Normally a general timer is valid, which means it can trigger or qualify an action. There is an action which can set the time for a timer. When set, the timer is invalid, so would de-assert or not qualify an action, and begins counting down its timer. When its timer expires, it goes valid again, so would assert or qualify another action.
Name		Program a text name of up to 32 characters in length. The name may be used to describe the purpose and/or period of this timer.

Calibrations

Entity/Feature	Option	Description
Calibration		Select the Calibration to program or edit.
Name		Program a text name of up to 32 characters in length.
Offset		Offset to add to Raw multiplied to Gain.
Gain		Factor by which the Raw value is multiplied.
Shift		Denominator (as a power of 2) for the Gain / Offset calculation.
Calibrate Calculation		This is the calculation that will be used in this Calibration. This equation is derived from the parameters programmed in the options above.
Effective Gain		The gain that would achieve the same result (without the shift).
Format / Scale		Used to determine how the analogue value is to be displayed. It includes the scaling, sign if required and text for the desired units. e.g. units = COMMON_UNIT_MILLIKELVIN and want to display between -30.0 and +10.0
Display String		Units or gauge ID test to display.
Minimum String		Minimum value in XXX.YYY format, matching scale_string.
Maximum String		Maximum value in XXX.YYY format, matching scale_string.



Inner Range Pty Ltd

ABN 26 007 103 933

1 Millennium Court, Knoxfield, Victoria 3180, Australia

PO Box 9292, Scoresby, Victoria 3179, Australia

Telephone: +61 3 9780 4300

Facsimile: +61 3 9753 3499

Email: enquiries@innerrange.com

Web: www.innerrange.com

