AN-334

Programming Guard Tours in Protege GX

Application Note

The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited, Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2021. All rights reserved.

Last Published: 22-Oct-21 10:57 AM

Contents

Introduction 4
Prerequisites 4
Scenario: Police Cellblocks 5
Programming Requirements 5
Creating Virtual Inputs and Outputs 6
Programming Areas and Doors 7
Adding the Areas 7
Programming the Inputs 8
Adding the Door Types 8
Programming the Doors 8
Programming Access and Output Control 10
Configuring the Reader Expander 10
Adding the Area Groups 10
Adding the Access Levels 11
Adding a User 11
Creating Programmable Functions 12
Testing the Operation 13
Running Event Reports 13
Optional: Prevent Guards from Silencing the Alarm 15
Adding the Schedules 15
Modifying the Checkpoint Access Levels 15
Creating the Supervisor User 15
Testing the Programming 16

Introduction

A guard tour is a method for ensuring that security guards complete a certain patrol route at the expected times. Guards must 'check in' at specific locations within defined intervals, and an alarm is raised if this does not occur. This ensures that high security areas are checked regularly, and produces a record for compliance and review purposes.

The flexibility of Protege GX enables you to extend your existing access and security system to provide custom guard tour functionality. Card readers installed at key locations provide the checkpoints, allowing guards to use their standard access cards to check in. The readers also provide useful feedback in the form of specific LED colors and beeper patterns to show when a check is due. Finally, all events are logged in Protege GX, making it simple to report on the guards' rounds.

This feature is applicable to many industries, including:

- Prisons and police facilities
- Banks and casinos with high security vaults
- Scientific facilities with a need to regularly check equipment
- Lone worker situations

Each guard tour setup will be unique, based on the needs of your site. This application note presents an example scenario, which can provide guidance for planning your own programming.

Prerequisites

The following components must be installed and operational.

Software	Requirements
Protege GX software	No specific version required.
Controllers	**Requirements**
PRT-CTRL-DIN	Area status LEDs may be used to activate warning and alarm colors on the card readers. This requires controller firmware version 2.08.883 or higher.
PRT-CTRL-DIN-1D	
Reader Expanders	**Requirements**
PRT-RDM2-DIN-485	No specific version required.
PRT-HRDM-DIN	
Card Readers	**Requirements**
tSec Readers	Area status LEDs require the following: • tSec Readers with RGB LEDs. • RS-485 reader connection. • tSec Reader firmware version 1.04.257 or higher. OSDP readers may also be used.

Scenario: Police Cellblocks

In this programming scenario we will program a police facility with two cellblocks, each of which must be inspected at least once every hour. Outside each cellblock is a 'checkpoint' card reader, which signals when an inspection is due. The checkpoint has three states, as indicated by the LED and beeper of the card reader:

- **Green, silent**: All clear, no inspection due
- **Orange flashing, periodic beeping**: Warning, inspection is due
- **Red, continuous beeping**: Alarm, inspection has not been completed
- **Orange flashing, silent**: Reset required, alarm has occurred
- **Blue, silent**: Disabled

The police facility requires the cells to be checked at least once every 45-60 minutes. When the checkpoint is activated it remains in the 'All clear' state for 45 minutes. It then changes to the 'Warning' state to show that an inspection is due. The officer has 15 minutes to complete the inspection and badge their card at the reader, returning the checkpoint to the 'All clear' state. If no officer badges at the reader during this time the checkpoint will go into the 'Alarm' state for 1 minute and an alarm will be raised in Protege GX.

Programming Requirements

Before you begin, it is assumed that you have a controller connected and online with Protege GX, and that the onboard reader expander is enabled (alternatively, you may use a separate reader expander). One card reader is required for each checkpoint that is programmed. A status page may also be useful for monitoring events.

As this scenario uses area status LEDs, ensure that you meet all of the requirements described in the Prerequisites (see previous page).

The following records will be programmed as part of this guard tour setup:

Record	Notes
Virtual input	1 per checkpoint
Virtual output	1 per checkpoint
Area	1 per checkpoint
Door type	1 per checkpoint
Door	1 per checkpoint
Area group	1 per checkpoint
Access level	1 per checkpoint
User	1 per guard/officer
Programmable function	2 per checkpoint
Event report	1 per checkpoint

Creating Virtual Inputs and Outputs

The guard tour programming requires one virtual input and one virtual output per checkpoint, which are used to automatically activate the alarm after the warning period expires. We will begin by programming these items so that they are available for use later.

Virtual inputs and outputs allow the controller to simulate binary states (open/closed, on/off) without a physical device connected.

Creating the Virtual Alarm Inputs

1. Navigate to **Expanders | Input expanders**.
2. Select the relevant **Controller** in the toolbar.
3. Click **Add** to create a new input expander record with the name Guard Tour (Virtual ZX248).
4. Enable the **Virtual module** option.
5. Set the **Physical address** to 248.
6. Click **Save**.
7. Set the **Type** to PRT-ZX16-DIN.
8. Disable the **Add trouble inputs** option.
9. Click **Add now**.
10. Navigate to **Programming | Inputs** to view the new virtual inputs.
11. Select the first input and name it Checkpoint 1 (Alarm). Click **Save**.
12. Select the second input and name it Checkpoint 2 (Alarm). Click **Save**.

Creating the Virtual Armed Outputs

1. Navigate to **Expanders | Output expanders**.
2. Select the relevant **Controller** in the toolbar.
3. Click **Add** to create a new output expander record with the name Guard Tour (Virtual PX32).
4. Enable the **Virtual module** option.
5. Set the **Physical address** to 32.
6. Click **Save**.
7. Disable the **Add trouble inputs** option.
8. Click **Add now**.
9. Navigate to **Programming | Outputs** to view the new virtual outputs.
10. Select the first output and name it Checkpoint 1 (Armed). Click **Save**.
11. Select the second output and name it Checkpoint 2 (Armed). Click **Save**.

Programming Areas and Doors

In this section, we will create and configure one area and one door for each checkpoint.

Adding the Areas

Each checkpoint will be represented by an area, which is used to track the status of the checkpoint.

Area Status	Checkpoint Status
Disarmed	All clear
Exit delay	Warning
Armed / Alarm activated	Alarm A programmable function will be used to cause the area to go into alarm as soon as it is armed.
Armed / Alarms in mem	Reset required

To create the checkpoint areas:

1. Navigate to **Programming | Areas**.
2. Add a new area with the name Checkpoint 1.
3. In the **Configuration** tab, set the following timings:
   - **Entry time**: 0
   - **Exit time**: 900

     Our scenario requires a warning time of 15 minutes (900 seconds). For testing purposes you can set this to a shorter time, e.g. 15s.
   - **Alarm 1 time**: 1
4. In the **Outputs** tab, set the following outputs:
   - **Bell output**: Reader 1 beeper
   - **Exit delay output**: Reader 1 beeper
   - **Exit delay pulse on time**: 1
   - **Exit delay pulse off time**: 19
   - **Armed output**: Checkpoint 1 (Armed)
5. Click **Save**.
6. Add a second area, then click **Copy**. Select Checkpoint 1 and click **OK** to copy the settings.
7. Rename the area Checkpoint 2. In the **Outputs** tab, change the **Bell output** to Reader 2 beeper and **Exit delay output** to Checkpoint 2 (Armed).
8. Click **Save**.
9. Take a note of the **Database ID** of each area.

Programming the Inputs

The virtual inputs created above will be used to put the checkpoint areas into alarm, so the areas must be assigned to their respective inputs.

1. Navigate to **Programming | Inputs** and select Checkpoint 1 (Alarm).
2. In the **Areas and input types** tab, select the following:
   - **Area 1**: Checkpoint 1
   - **Input type 1**: Instant
3. Click **Save**.
4. Select Checkpoint 2 (Alarm).
5. In the **Areas and input types** tab, select the following:
   - **Area 1**: Checkpoint 2
   - **Input type 1**: Instant
6. Click **Save**.
7. Return to **Programming | Areas**. Right click on each area and click **Arm**.

Adding the Door Types

For each checkpoint, we will program one door type to control the LED pattern for each status.

1. Navigate to **Programming | Door types**.
2. Add a new door type called Checkpoint 1 (LED Patterns).
3. Scroll down and expand the **Commands** section.
4. Enter the following commands on separate rows:

   ```
   LED_FUNC[0]=1,X,3,1,1,1,0
   LED_FUNC[1]=1,X,2,3,0,5,5
   ```

   Replace **X** with the Database ID of the Checkpoint 1 area.

   These commands can be customized to meet the requirements for your site. For more information about area status LED functions, see Application Note 271: Configuring Area Status LED Functions.
5. Click **Save**.
6. Click **Add**, then click **Copy**. Select Checkpoint 1 (LED Patterns) and click **OK**.
7. Change the name to Checkpoint 2 (LED Patterns).
8. In the **Commands** field, change the Database ID in each command to that of Checkpoint 2.
9. Click **Save**.

Programming the Doors

Door records are used to represent the card readers which are associated with each checkpoint. In this scenario, the card readers are only used for the guard tour functionality, not to control physical doors.

1. Navigate to **Programming | Doors**.
2. Select or add the door connected to reader port 1 and name it Checkpoint 1 Reader.
3. Set the **Door type** to Checkpoint 1 (LED Patterns).
4. Set the **Area inside door** to Checkpoint 1.

5. As this reader port is not used to control a physical door, you can remove any unnecessary physical devices in the **Outputs** and **Inputs** tabs.
6. Click **Save**.
7. Select the door connected to reader port 2 and name it Checkpoint 2 Reader.
8. Set the **Door type** to Checkpoint 2 (LED Patterns).
9. Set the **Area inside door** to Checkpoint 2.
10. Remove any unnecessary outputs and inputs.
11. Click **Save**.

Programming Access and Output Control

When an officer badges their card at the checkpoint reader, two things must happen:

- The checkpoint area must be disarmed, putting the checkpoint in the 'All clear' state.
- The green LED on the reader must be activated. This is used both to display the 'All clear' status on the reader and to control the timing of the area arming.

To achieve these, we must configure the reader expander and create an appropriate access level for each checkpoint.

Configuring the Reader Expander

Some reader expander configuration is required to allow users to disarm the checkpoint area and activate an output when they badge a card at the reader.

1. Navigate to **Expanders | Reader expanders** and select the reader expander which is controlling the guard tour.
2. In the **Reader 1** tab, enable the following options:
   - **Disarm area for door on access**
   - **Activate access level output**
3. Enable the same options in the **Reader 2** tab.
4. Click **Save**.
5. Wait for the changes to be downloaded to the controller, then right click on the reader expander record and click **Update module**.

Adding the Area Groups

To provide officers with access to disarm the checkpoint areas, appropriate area groups must be created.

1. Navigate to **Groups | Area groups**.
2. Add an area group with the name Checkpoint 1 Group.
3. Click **Add** and select Checkpoint 1. Click **OK**.
4. Click **Save**.
5. Repeat to create the Checkpoint 2 Group.

Adding the Access Levels

When programming a guard tour with multiple checkpoints, it is necessary to create one access level per checkpoint. This is because each checkpoint has a unique green reader LED output which must be activated when the access level is used.

1. Navigate to **Users | Access levels**.
2. Add a new record called Checkpoint 1 Inspection.
3. Set the **Time to activate output** to 2700.

   Our scenario requires the checkpoint to remain in the 'all clear' state with the green LED activated for 45 minutes (2700s). For testing purposes you can set this to a shorter time, e.g. 45s.
4. Enable the **Reader access activates output** option.
5. In the **Doors** tab, add Checkpoint 1 Reader.
6. In the **Disarming area groups** tab, add Checkpoint 1 Group.
7. In the **Outputs** tab, add the reader 1 green LED.
8. Click **Save**.
9. Add a new access level called Checkpoint 2 Inspection.
10. Set the **Time to activate output** to 2700 (or 45 for testing).
11. Enable the **Reader access activates output** option.
12. In the **Doors** tab, add Checkpoint 2 Reader.
13. In the **Disarming area groups** tab, add Checkpoint 2 Group.
14. In the **Outputs** tab, add the reader 2 green LED.
15. Click **Save**.

Adding a User

We will add a user so that we can test our programming. This officer will have access to both checkpoints.

1. Navigate to **Users | Users** and add a new user record.
2. Name the user Police Officer.
3. Assign the user an access card.
4. In the **Access levels** tab, add both Checkpoint 1 Inspection and Checkpoint 2 Inspection.
5. Click **Save**.

At this stage, you should test the system to make sure that the programming we have done so far is working as expected.

1. Badge the officer's card at reader 1.
   - The Checkpoint 1 area should disarm.
   - The reader 1 green LED should turn on for 45 seconds.
2. Arm the Checkpoint 1 area using the software.
   - The reader LED should display flashing orange.
   - During the 15 second exit delay, the reader beeper should beep periodically.
   - When the area is fully armed, the Checkpoint 1 (Armed) output should be activated.
3. Repeat the above steps to test checkpoint 2.

Creating Programmable Functions

For each checkpoint, two programmable functions are required:

- An area control programmable function to arm the checkpoint area when the reader green LED output turns off. This means that the warning period begins after the output's activation time expires.
- An input follows output programmable function to activate the virtual input as soon as the checkpoint area finishes arming. This means that when the warning period finishes, the alarm will start immediately.

Adding the Area Control Programmable Functions

1. Navigate to **Automation | Programmable functions**.
2. Select the relevant **Controller** in the toolbar.
3. Add a new programmable function with the name Checkpoint 1 Area Control.
4. Set the **Type** to Area control.
5. In the **Area control** tab, set the following:
   - **Area function**: 4 - Area arms on output turning off
   - **Output to check**: Reader 1 green LED
   - **Area to control**: Checkpoint 1
6. Click **Save**.
7. Add a new function called Checkpoint 2 Area Control, using the relevant records for checkpoint 2.
8. Click **Save**.

Adding the Input Follows Output Programmable Functions

1. Add a new programmable function with the name Checkpoint 1 Input Follows Output.
2. Set the **Type** to Input follows output.
3. In the **Input follows output** tab, set the following:
   - **Input follows output**: Checkpoint 1 (Alarm)
   - **Output to follow**: Checkpoint 1 (Armed)
4. Click **Save**.
5. Add a new function called Checkpoint 2 Input Follows Output, using the relevant records for checkpoint 2.
6. Click **Save**.
7. Wait for the changes to be downloaded to the controller, then right click on each programmable function and click **Start**.

Testing the Operation

To test the operation of the guard tour, complete the following steps:

1. Badge the card assigned to the officer at the checkpoint 1 reader. The checkpoint is now in the 'All clear' state.
   - The reader LED should display green.
   - The Checkpoint 1 area should be disarmed.
2. After 45 seconds, the checkpoint should change to the 'Warning' state.
   - The reader LED should display flashing orange.
   - The reader beeper should beep periodically.
   - The Checkpoint 1 area should be in exit delay.
3. Badge the card again. The checkpoint should return to the 'All clear' state.
4. This time, wait for 60 seconds without badging the card. After a 15 second warning, the checkpoint should change to the 'Alarm' state.
   - The reader LED should display red.
   - The reader beeper should beep continuously.
   - The Checkpoint 1 area should be in alarm.
5. After 1 minute, the checkpoint should change to the 'Reset required' state.
   - The reader LED should display flashing orange.
   - The reader beeper should be silent.
   - The Checkpoint 1 area should be armed with alarms in memory.
6. To reset the checkpoint, badge the officer's card again. The cycle will then repeat.
7. To disable the checkpoint, disarm the checkpoint area using another method, e.g. through the software.
8. Repeat these tests for checkpoint 2.

Running Event Reports

One of the main priorities of a guard tour system is accurate reporting to confirm that all checkpoints were checked at the correct intervals and highlight any missed checks. This is easy to achieve using event reports.

Creating Event Filters

1. Navigate to **Events | Event filters**.
2. Click **Add** and name the event filter Checkpoint 1 Events.
3. In the **Event types** tab, disable the **Include all event types** checkbox.
4. Click **Add**, then select the following events from the **All Area Events** section:

Event	Checkpoint State
Area <AREA_NAME> Alarm Activated	The checkpoint has entered 'Alarm' state.
Area <AREA_NAME> Arming Cancelled By <USER_NAME> At <DOOR_NAME>	The checkpoint has been reset before the alarm is activated.
Area <AREA_NAME> Arming Started By System Using <USER_NAME>	The checkpoint has entered 'Warning' state.

Event	Checkpoint State
All events of the form: Area <AREA_NAME> Disarmed By...	Including all disarm events allows you to record when the checkpoint has been disabled (by disarming through a method other than the card reader).

5. In the **Records** tab, click the **Add** button for the first record filter.
6. Set the **Device type** to Area.
7. Select Checkpoint 1, then click **OK**.
8. Click **Save**.
9. Repeat to create an event filter for Checkpoint 2.

Creating Event Reports

1. Navigate to **Reports | Setup | Event**.
2. Click **Add** and name the new report Checkpoint 1 Report.
3. Under **Event filters**, select the All Events filter and click **Delete**.
4. Click **Add**.
5. Set the **Event filter** to Checkpoint 1&2 Events and enable **Access all record groups**.
6. Click **OK**.
7. If desired, use the **Columns** tab to customize which columns will be displayed in the report.
8. Click **Save**.
9. Repeat to create a Checkpoint 2 Report.
10. To run the reports, navigate to **Reports | Event**.
11. In the toolbar, set the **Event report** to Checkpoint 1 Report and click **Execute**.
12. Set the **Period** as appropriate, and click **OK**.
13. The report will show the relevant events for the checkpoint, providing proof that it has been checked at the correct times. Repeat to view the report for Checkpoint 2.

You can use the **Export** and **Email** tabs in the event report setup to automatically save and/or send the reports regularly.

Optional: Prevent Guards from Silencing the Alarm

On some sites, there may be a requirement to prevent security guards or officers from resetting the checkpoints after an alarm. Instead, the checkpoints can only be reset by a supervisor.

To achieve this, we can program a schedule that is valid only when the checkpoint's **Armed output** is off. This is set on the area group in the access level programming. We will also create a supervisor access level which can reset the checkpoints.

Adding the Schedules

For each checkpoint we must create a schedule which is valid 24/7 except when the checkpoint is armed (i.e. in the 'Alarm' or 'Reset required' states).

1. Navigate to **Sites | Schedules**.
2. Click **Add** and name the new schedule Checkpoint 1 All Clear / Warning.
3. Enable **Period 1** for all days of the week.
4. Set the **Holiday mode** for Period 1 to Ignore Holiday.
5. In the **Options** tab, enable **Validate schedule if qualify output off**.
6. Set the **Qualify output** to Checkpoint 1 (Armed).
7. Click **Save**.
8. Repeat to create the Checkpoint 2 All Clear / Warning schedule.

Modifying the Checkpoint Access Levels

Now we must edit the checkpoint access levels created above so that users are only allowed to disarm the checkpoints before they enter the 'Alarm' state.

1. Navigate to **Users | Access levels**.
2. Select Checkpoint 1 Inspection.
3. In the **Disarming area groups** tab, set the **Schedule** for the area group to Checkpoint 1 All Clear / Warning.
4. Click **Save**.
5. Repeat for the Checkpoint 2 Inspection access level.

Creating the Supervisor User

The supervisor user will have access to disarm both checkpoints at all times.

1. Still in **Users | Access levels**, click **Add** and name the new access level Checkpoint Supervisor.
2. In the **Doors** tab, add both Checkpoint 1 Reader and Checkpoint 2 Reader.
3. In the **Disarming area groups** tab, add both Checkpoint 1 Group and Checkpoint 2 Group.
4. Click **Save**.
5. Navigate to **Users | Users**.
6. Add a new user called Police Supervisor.
7. Assign the user an access card.

8. In the **Access levels** tab, add the Checkpoint Supervisor access level.
9. Click **Save**.

Testing the Programming

To test the programming, enable the checkpoints and wait until the alarm is activated (red LED, beeper activated).

1. Badge the Police Officer's card and observe that access is denied and the checkpoint does not reset.
2. Wait until the alarm times out and the checkpoint enters 'Reset required' state (orange flashing, no beeper). Badge the Police Officer's card again and observe that access is still denied.
3. Now badge the Police Supervisor's card. Access is granted, and the checkpoint enters the 'Disabled' state (blue LED, no beeper).
4. Badge the Police Officer's card again. This time access is granted and the checkpoint enters 'All clear' state (green LED, no beeper).

In this configuration, the supervisor can disarm the checkpoint area, but does not activate the green LED output. i.e. the checkpoint does not start the guard tour again until an officer badges their card. If the supervisor is required to restart the checkpoint, you will need to create a separate supervisor access level for each checkpoint.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2021. All rights reserved.

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.