

# SIEMENS



## **Siveillance Intrusion Pro— Integration into Desigo CC Operation Manual**

Data and design subject to change without notice. / Supply subject to availability.

© 2024 Copyright by Siemens AG

We reserve all rights in this document and in the subject thereof. By acceptance of the document the recipient acknowledges these rights and undertakes not to publish the document nor the subject thereof in full or in part, nor to make them available to any third party without our prior express written authorization, nor to use it for any purpose other than for which it was delivered to him.

# Content

- 1      About this Document ..... 8**
  - 1.1    Further Documentation ..... 8
- 2      Safety ..... 9**
  - 2.1    Target Audience ..... 9
  - 2.2    General Safety Instructions ..... 9
  - 2.3    Meaning of Symbols ..... 9
- 3      General Information..... 10**
  - 3.1    Terms of Use for Documentation ..... 10
  - 3.2    Supplementary Agreement for the Provision of Documentation ..... 10
- 4      Operation/Use of the Siveillance Intrusion Integration ..... 11**
  - 4.1    Visualization of Area / Detector / Hardware Module States ..... 11
    - 4.1.1.1    Areas ..... 11
    - 4.1.1.2    Hardware Components..... 12
    - 4.1.1.3    Detectors ..... 13
  - 4.2    Alarms and Notifications ..... 13
    - 4.2.1    Alarms / Notifications in the Event of a Connection Interruption and a Change of Configuration..... 13
    - 4.2.2    Alarming of Detectors and Hardware Modules ..... 13
    - 4.2.3    License Warnings and Errors ..... 14

# Copyright

Copyright © 2023. Siemens AG. All rights reserved.

The information contained in this publication is company-proprietary to Siemens AG. This publication and related software are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright law. Reverse engineering / copying of any Siemens AG hardware, software, documentation, or training materials is strictly prohibited.

This publication and related software remain the exclusive property of Siemens AG. No part of this publication or related software may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission from Siemens AG.

Due to continued product development, the information in this publication and related software may change without notice. Please report any errors to Siemens AG in writing. Siemens AG does not warrant that this publication or related software is error-free.

Any references to companies or persons are for purposes of illustration only and are not intended to refer to actual individuals or organizations.

## Cyber security disclaimer

Siemens provides a portfolio of products, solutions, systems and services that includes security functions that support the secure operation of plants, systems, machines and networks. In the field of Building Technologies, this includes building automation and control, fire safety, security management as well as physical security systems.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art security concept. Siemens' portfolio only forms one element of such a concept.

You are responsible for preventing unauthorized access to your plants, systems, machines and networks which should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. Additionally, Siemens' guidance on appropriate security measures should be taken into account. For additional information, please contact your Siemens sales representative or visit <http://www.siemens.com/industrialsecurity>.

Siemens' portfolio undergoes continuous development to make it more secure. Siemens strongly recommends that updates are applied as soon as they are available and that the latest versions are used. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats. Siemens strongly recommends to comply with security advisories on the latest security threats, patches, and other related measures, published, among others, under

For additional information on building technology security and our offerings, contact your Siemens sales or project department. We strongly recommend signing up for our security advisories, which provide information on the latest security threats, patches and other mitigation measures.

<http://www.siemens.com/cert/de/cert-security-advisories.htm>

## **Trademarks**

Designo CC™ und Siveillance Intrusion PRO/ADV™ are a registered trademark of Siemens AG.

All other product or company names mentioned in this document are trademarks or registered trademarks of their respective owners and are used only for purposes of identification or description.

## **Contact**

If you have questions or suggestions regarding the product or this documentation, please approach your Siemens correspondent:


Edition: 28.05.2024 v6.0.145.0, v7.0.0002.9, v8.0.0001.1

## Glossary of Terms, Abbreviations and Acronyms

<b>Areas</b>	Area types which are supported by Siveillance Intrusion Pro and displayed as “areas” within DCC, such as intrusion areas, doors, “On-Off-Areas”, lock area or generic areas.
<b>Control, to control</b>	To operate, command, execute.
<b>Control panel</b>	Control unit or system in use such as “Siveillance Intrusion panel” / Siveillance Intrusion control panel.
<b>DAIG</b>	short for “Desigo Application Integration Germany”, an additional DCC-EM (extension module) providing the infrastructure and common basis for the integration of subsystems into DCC.
<b>DCC</b>	Short for „Desigo CC”
<b>Desigo CC</b>	Siemens integrated building management platform for managing buildings
<b>Intrusion area</b>	A single zone or multiple zones.
<b>I/O module</b>	Input/Output module, transferring data from one device to another
<b>On-/Off areas</b>	One or multiple outputs within Siveillance Intrusion Pro.
<b>Silnt</b>	Short for the Siemens intrusion detection system “Siveillance Intrusion Pro”
<b>Silnt-integration</b>	An integration of Siveillance Intrusion Pro into the Siemens management system platform Desigo CC (DCC), also referred to as an interface or link to DCC.
<b>“Ready to Set” command</b>	Ready to be locked, condition met is ok be locked.
<b>State</b>	Refers to a status or condition.
<b>Unset/set, to unset/set</b>	To arm or disarm.

# 1 About this Document

This document describes to the respective commissioning personnel, how to operate and to use the Siveillance Intrusion Pro (Silnt)-integration linking the intrusion detection system Siveillance Intrusion PRO/ADV (former Transliner Pro, hereafter referred to as Siveillance Intrusion Pro, or short "Silnt") to the Siemens management system platform Desigo CC (DCC).

	<p><b>PLEASE NOTE</b></p> <p>Both the installation and configurational set up of the integration are described in an an independent document named "EXT_ENG_049_SiveillanceIntrusionPro-DCC-Administration-Manual_01.pdf".</p>
---	--

## 1.1 Further Documentation

- EXT\_ENG\_049\_SiveillanceIntrusionPro -DCC-Administration-Manual\_01.pdf
- Desigo CC 6.0 Operating Help
- Desigo CC 6.0 Engineering Help

# 2     Safety

## 2.1    Target Audience

This document provides instructions for the following target readers:

Target group	Qualification	Activity	Condition of the Product
Operation personnel	Has Desigo CC knowledge in operating the system.	Confirms alarms/notifications which are which are generated by the Silnt-integration. Controls the operation of Silnt. Monitors/supervises the overall system state.	Fully configured integration/interface.

## 2.2    General Safety Instructions

Please note all instructions in this manual.

- Retain this document for reference purposes
- Always include this document with the product if it is transferred to a new owner

### Loss of data when updating the software

Secure all your data before updating the software.

## 2.3    Meaning of Symbols



Tips and information.

	<b>PLEASE NOTE</b>
	Includes additional information to a certain subject.



## 3 General Information

### 3.1 Terms of Use for Documentation

This documentation has been carefully tested for compliance with the hard- and software components described.

However, discrepancies between the documentation and the software cannot be fully excluded. Therefore, we do not accept any liability for exact compliance.

The information in this guide is verified on a regular basis and any required corrections will be included in subsequent editions. We are always grateful for your user feedback and suggested corrections.

Please note, that the subsequently outlined supplementary agreement for the provision of RC-DE SI SSP documentation is applicable.

### 3.2 Supplementary Agreement for the Provision of Documentation

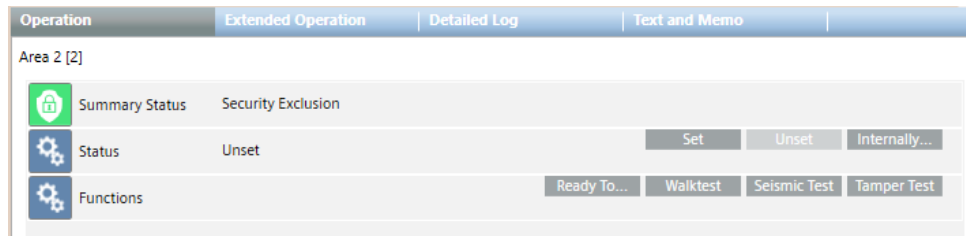
- You have the perpetual and non-exclusive right to partly modify, reproduce in an altered or unaltered manner and transfer either on paper or another data storage medium to third parties as part of this manual (subsequently referred to as administration manual) for the purpose of generating technical documents of systems which are equipped with the SI SSP DE software extension module DAIG-TrPro.
- If adding other documentation into this administration manual and if any further document processing is done, please make sure that all safety -relevant instructions are maintained and kept visible.
- You have the sole responsibility for all included, unaltered or altered documentation.
- Reproduction and duplication of this documentation as well as the use and communication of its content is not permitted unless specifically approved.
- Do not delete Siemens copyright notes from the documentation.
- Document modifications must be pointed out accordingly, for example by an additional copyright notice.
- You are not authorized to use the company brand name SIEMENS.
- If using SIEMENS trademarks/brands in the administration manual, you must add a reference about this accordingly (for example by adding a note stating "...is a registered trademark (or brand) of SIEMENS AG")
- Contravention commits to compensation. All rights reserved, especially if a patent is granted, or the product is GM registered.

## 4 Operation/Use of the Siveillance Intrusion Integration

### 4.1 Visualization of Area / Detector / Hardware Module States

After successful configuration of a Silnt-device in Desigo CC, the corresponding tree nodes for areas, detectors, and hardware modules will be displayed in the tree-view of the DCC management-view:

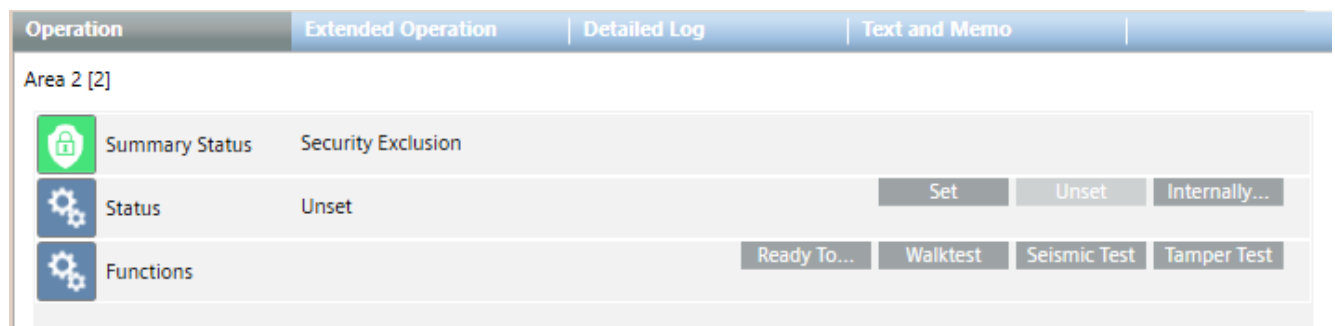
The operation pane will show the state of the individual tree-node-items and the available command/control options. Please see below an example for “intrusion area”:



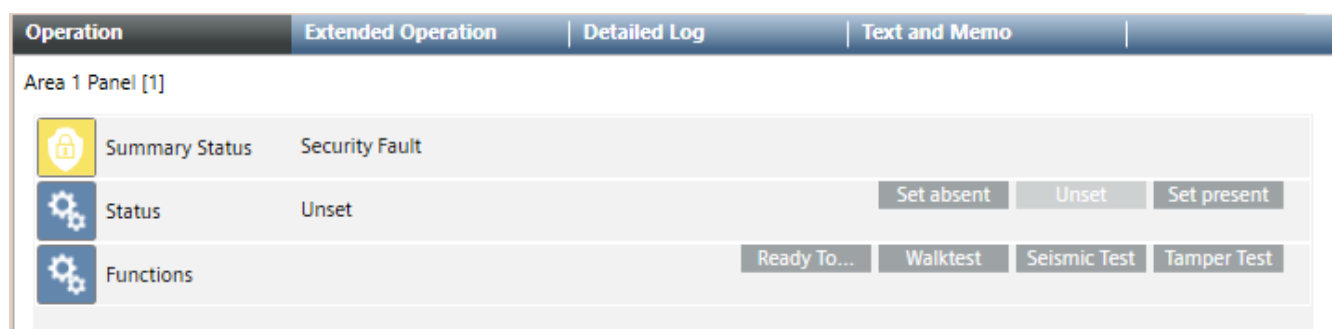
The commands are context-sensitive having only those command-buttons activated that are possible for the current state.

#### 4.1.1.1 Areas


An area state is displayed in accordance with the one transferred from the Silnt-system. The area type determines the available command/control options.




State/Status & Control of an Intrusion Area





State/Status & Control of a Present/Absent Area

Operation	Extended Operation	Detailed Log	Text and Memo
Door1 [4]			
	Status	Closed	<input type="button" value="Open"/> <input type="button" value="Close"/> <input type="button" value="Open Temp."/>


State/Status & Control of Doors

Operation	Extended Operation	Detailed Log	Text and Memo
Random alarms [7]			
	Status	On	<input type="button" value="On"/> <input type="button" value="Off"/>

State/Status & Control of On-/Off-Areas

Operation	Extended Operation	Detailed Log	Text and Memo
Perimeter [8]			
	Summary Status	Security Exclusion	
	Status	PL0: Unset	<input type="button" value="PL0 Unset"/> <input type="button" value="PL1 Set"/> <input type="button" value="PL2 Set"/> <input type="button" value="PL3 Set"/>

State/Status & Control of Perimeter Areas

Operation	Extended Operation	Detailed Log	Text and Memo
System [9]			
	Status	Unset	<div> <input type="button" value="Send"/> </div> <div> <input type="button" value="Internally Set"/> <input type="button" value="Seismic Test"/> <input type="button" value="Set"/> <input type="button" value="Set present"/> <input type="button" value="Tamper Test"/> <input type="button" value="Walktest"/> </div>



State/Status & Control of Generic Areas

#### 4.1.1.2 Hardware Components

A hardware component aggregates multiple inputs. Therefore, the state of a hardware component is an aggregated one displaying the input type of the most critical input, which was triggered.

For example, if PS5 triggers both the “open” input and the “power failure” one at the same time, a threat will be considered more critical and the system’s aggregated state equals “Danger/Threat”.

The hardware components can either be switched off or on by the “Mode”-function. This applies to all inputs for the corresponding hardware component.

Operation	Extended Operation	Detailed Log	Text and Memo
Power supply [3000_PS5]			
 Status	Normal		
 Function	Included		<input type="button" value="Include"/> <input type="button" value="Exclude"/>




Aggregated Status/State and Command/Control of a HW-Component

### 4.1.1.3 Detectors

A detector aggregates multiple inputs. Therefore, the state of a detector is an aggregated one, displaying the most critical alarm type which was triggered.

The physical state combines the physical states of the detector inputs (closed, open, etc.) to an aggregated state which e.g., considers “Sabotage” as more critical than “Open”.

The “Mode”-function allows the detectors to be switched off or on. This control-option applies to all inputs of the relevant detector.

Operation	Extended Operation	Detailed Log	Text and Memo
Motion sensor2 [123456110]			
 Status	Normal		
 Physical Status	Open		
 Function	Included		<input type="button" value="Include"/> <input type="button" value="Exclude"/>

Aggregated Status/State, Physical Status/State and Command/Control of a Detector

The command & control-functions are not directly executed on the datapoints for the respective state/status. Instead, these are forwarded to the Silnt-system. Resulting changes for the status/state will again be transferred from the Silnt-system to DCC and displayed there accordingly,


If the change for a status/state is not successful, (for example, in the event of setting an intrusion area), the status/states must not switch to the desired target- status/state. For this reason, a corresponding message/notification will be created being displayed in the category “information”.


## 4.2 Alarms and Notifications

### 4.2.1 Alarms / Notifications in the Event of a Connection Interruption and a Change of Configuration

### 4.2.2 Alarming of Detectors and Hardware Modules

The alarms/notifications generated by Silnt will be recorded into the corresponding categories in accordance with the alarm tables used.

Depending on the alarm table-configuration, an alarm must either be acknowledged/confirmed (  ) (meaning the user must take action in the DCC-alarm list) or it will be auto-acknowledged/confirmed (meaning no action by the user must be taken by the user and the alarm disappears as soon as it is reset by Silnt).

Some alarms can be reset by the DCC-user as well (  ). In this event a reset-command, resetting the alarm, will be sent to the Silnt-system, provided that Silnt does allow his resetting action. If Silnt rejects the alarm-reset, it will remain in the current status/state.

Also, please refer to the administration manual to view the alarm-/state-changes, that are possible.

### 4.2.3 License Warnings and Errors

If there is no valid Silnt-system-license (please refer to the administration manual), the Silnt-integration/interface will switch to a 30-day-trial version. A license warning message will be displayed in the Alarm Manager accordingly.

After expiration of the 30-day-trial period this license warning will become a license error terminating the Silnt-integration/interface. This means, that no data from the Silnt-system will neither be received, nor alarms will be generated or reset.

By activating a valid license, the normal operating mode of the Silnt integration/interface will be established.