SIEMENS

Siveillance Intrusion Pro – Integration into Desigo CC Administration Manual

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

Content

Copyright

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

Desigo 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

Areas
Area types which are supported by Siveillance Intrusion Pro and displayed as “areas” within DCC, such as standard areas, doors, “On-Off-Areas”, lock area or generic areas.

Client Certificate
A type of digital certificate that is used by client systems to make authenticated requests to a remote server.

Control, to control
To operate, command, execute.

Control panel
Control unit or system in use such as “Siveillance Intrusion panel” / Siveillance Intrusion control panel.

DAIG
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.

DCC
Short for „Desigo CC”

Desigo CC
Siemens integrated building management platform for managing buildings

Intrusion area
A single zone or multiple zones.

I/O module
Input/Output module, transferring data from one device to another

LSN / LSN HW modules
Short for Local Security Network (German: Lokales Sicherheits-Netzwerk),

LSN gateway
applying networking technologies via LSN HW modules, LSN gateways, etc.

On-/Off areas
One or multiple outputs within Siveillance Intrusion PRO/ADV.

SiInt
Short for the Siemens intrusion detection system “Siveillance Intrusion Pro” (former name: “Guarto3000”-system)

Siveillance Intrusion Pro Integration / SiInt-integration
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.

PuTTY/Puttygen
A free and open-source terminal emulator, serial console, and network file transfer application. It supports several network protocols, such as SSH.

Private key file

A text file used initially to generate a Certificate Signing Request (CSR), and later to secure and verify connections using the certificate created per that request.

“Ready to Set” command

Ready to be locked, condition met is ok be locked.

SSH (access)

Short for Secure Shell, an encrypted network communication protocol used to secure the connection between Siveillance Video and Intrusion

SSH-user

Name of the user, whose credentials are a used for the SSH connection

State

Refers to a status or condition.

Guarto3000

Former name of the current Swiss Siveillance Intrusion Pro (short: SiInt-system)

Unset/set, to unset/set

To arm or disarm.

VdS

Short for „Verband der Sachversicherer“ or „Verband der Schadenversicherer“, a fully owned subsidiary of the German Insurance Association (GDV), one of Germany’s leading independent testing institutions for fire safety and security providing essential standards in safety and security solutions.

1 About this Document

This document describes to the respective commissioning personnel, how to set-up and configure the Swiss Siveillance Intrusion Pro to the Siemens management system platform Desigo CC (DCC).

!	***PLEASE NOTE***
	Because of differences in area configuration, states, alarming behavior and look, you have to integrate the Swiss Siveillance Intrusion Pro (formerly known as Guarto3000) by using the DAIG_Guarto3000_049-EM (described in this manual). If you want to integrate a Siveillance Intrusion Pro/Adv (**EU-Template**) or Siveillance Intrusion Pro/Adv (**DE-Template, formerly known as Transliner Pro**), please contact your regional Desigo CC portfolio manager. There is a separate EM for this case.

!	***PLEASE NOTE***
	SiInt establishes a connection to DCC by using the infrastructure of DAIG (Desigo Application Integration Germany). Therefore, as a prerequisite, before establishing a link to DCC, the following two action steps must be taken first: • The DAIG extension module must be installed. • The DAIG-driver as well as the DAIG-network-tree-nodes must be created and configured. Please perform these steps in accordance with the DAIG administration manual, which usually is delivered with the DAIG EM.
!	***PLEASE NOTE***
	This document only describes the installation and configurational set up of the SiInt-integration. The operation of the integration is described in an independent document named “EXT_OPR_049_SiveillanceIntrusion-DCC-Operation_Manual_01.pdf”. This document is made available by the DCC-support/online help.

Please perform the following steps to set up the integration/EM:

- Customize the SiInt-configuration to enable access by Desigo CC (DCC)
- Install the des DAIG_TrPro_049- extension module
- Create and install a certificate to facilitate an encrypted communication between the DCC DAIG Driver and SiInt
- Configure/set up the Siveillance Intrusion connection in DCC
- Import the SiInt-configuration into DCC

Once successfully configured, set-up and started, the status for all intrusion objects from SiInt (such as areas, detectors, etc.) will be displayed in DCC. Objects are now allowed to be controlled and upcoming intrusion alarms and alert messages will be displayed in the DCC-alarm list.

1.1 Further Documentation

- EXT_ENG_049_DAIG-Administration_Manual_01.pdf
- EXT_OPR_049_Siveillance-Intrusion-PRO-ADV-DCC-Operation-Manual_0.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 Readers	Qualification	Activity	Condition of the Product
System Administrator / Data Entry & Maintenance	Has specialized knowledge in IT-systems, management systems and subsystems. Specific product training is required.	Configures and manages (user-) settings. Responsible for user management.	Integration/EM and connection ready for operation.
Commissioning/ maintenance personnel	Has specialized knowledge in IT systems, management systems and subsystems. Specific product training is required.	Installs and configures the SiInt integration/connection to DCC. Periodically checks on proper functional capability of the system, keeps the system up to date and manages the extension of the system.	Desigo CC and SiInt are installed and configured.
Operating personnel	Has basic Desigo CC knowledge on how to operate the system.	Confirms alarms/notifications which are which are generated by the SiInt-integration. Controls the operation of Siveillance Intrusion. Monitors/supervises the overall system state.	The integration/EM is configured.

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

ℹ	Tips and Information.

!	***PLEASE NOTE***
	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 System Outline

4.1 Overview

The Siveillance Intrusion PRO/ADV (SiInt) integration module establishing the connection to Desigo CC (DCC) will be delivered and provided as three different DCC extension modules (DAIG, DAIG_TrPro, TranslinerLib). These must be installed in addition to DCC.

During the installation process, the following components are made available:

- Desigo Object Modell for SiInt (Library)
- DCC-SW-interfaces to configure & operate the SiInt-integration (Snap-Ins)
- DCC-Driver including SiInt-modules to communicate with the SiInt-system (datapoints, command & control functions, alarms)

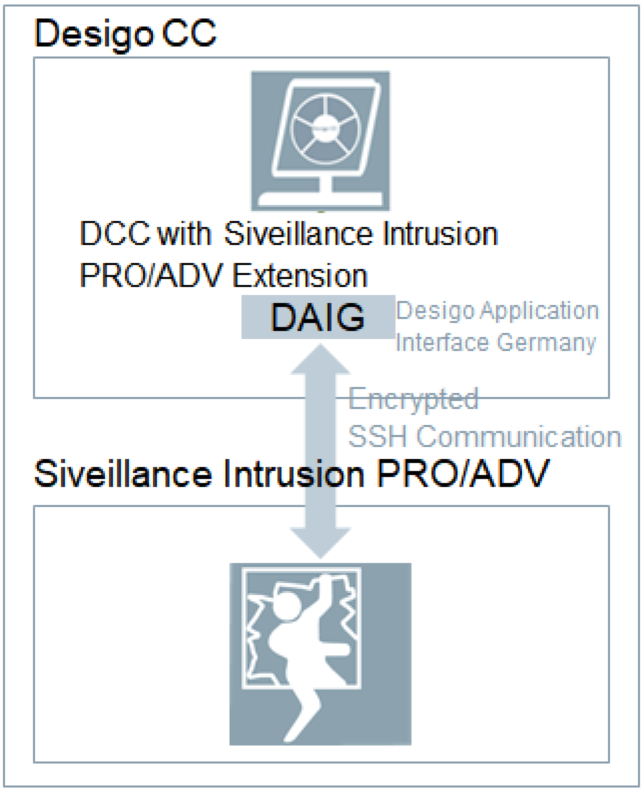

Desigo CC
DCC with Siveillance Intrusion PRO/ADV Extension
DAIG
Desigo Application Interface Germany
Encrypted SSH Communication
Siveillance Intrusion PRO/ADV

Figure 1: Connecting Siveillance Intrusion PRO/ADV (SiInt) to Desigo CC (DCC)

The installation and configuration of the SiInt-system is **not** part of this documentation. Please refer to chapter 5 for information on the required modifications that must be applied to the configuration of the SiInt-system.

4.2 Siveillance Intrusion PRO/ADV (SiInt) Object Modell

4.2.1 Hierarchy / Structure

DCC will display all intrusion elements, such as areas, hardware components and detectors.

Please see below the area types which are supported by SiInt. These will be visualized in DCC as areas having the following names:

- Intrusion areas
- Doors
- On-/Off areas
- Perimeter areas (type 1 and 2, see below)

- Generic areas

The following item types are displayed as hardware components:

- SiInt-units refer to main components and hardware modules, which can be created/set by the SiInt-configuration
- Hardware modules that are connected to the LSN

The detectors displayed include all devices,

- which are connected to the LSN as an independent address element.
- which are connected via LSN-HW modules.
- which are connected via I/O modules of the SiInt-bus connector.

4.2.1.1 Areas

Areas as well as their assigned detectors can be transferred one-to-one from the SiInt-configurational set-up. The structural information needed for this process will be transmitted via the SiInt-integration.

The SiInt-area types (intrusion areas, doors, On-/Off areas etc.) determine an area's type and consequently specify its visualization (icons), its control options and its alarming.

Area types which have not been modelled explicitly will be modelled as generic areas supporting the dynamic scalability of the SiInt-system.

4.2.1.2 Hardware Components and Detectors

To facilitate a user-friendly operation of the SiInt-integration within DCC, a detector-based SiInt-model must be built from the existing input-based model.

For this purpose, the following factors play a significant role:

- Assignment of inputs to hardware components and detectors
- Different hardware component types and alarms which can be triggered by their inputs
- Different detector types and alarms which are (or can) be triggered by the detectors

Assignment of inputs to hardware components and detectors

The following mechanisms are involved to enable a structural setup of the hardware components and detectors by means of their inputs, which are used to connect these devices to the system:

- The structural information of a hardware component is static and determined by the SiInt-configuration (for example PS5 having a defined number of inputs and input types). This also applies to hardware modules, which are connected via LSN
- The SiInt-interface transfers the process of assigning inputs to a specific detector, which functions as an addressing element being is directly connected to the LSN bus.
- The process of assigning inputs to a specific detector is automatically determined by a template (comment field) during the SiInt-configuration setup procedures (please refer to the next section for more details).
- The process of assigning the inputs to a detector will be defined manually by means of a comment field during the system supply procedures (please refer to the next section for more details).

Assignment of inputs to a specific detector via the SiInt-comment fields

Inputs which cannot be automatically assigned to a certain detector by means of their address data can be set and structured by the comment fields within the SiInt-configuration.

Please distinguish the following two events:

1. The need to manually (re-)configure structural information for existing installations. This can be done by means of the comment fields.

2. Automatic configuration in the event of new installations. In this case the new SiInt-templates will pre-fill the corresponding comment fields.

The following information can be entered into the comment fields:

- @@ID:x@@ Structural information: all inputs with same ID on the same hardware module will be combined into one detector.
  @@T:x@@ Type information: If an input of a detector is tagged with this type-information, a corresponding assignment of actual types to this detector will occur. This will lead to a distinguished means of visualization via icons within DCC (icons). The following types will be supported:
  - PIR: Motion detection
  - FIRE: Fire detection
  - GLASS: Glass break sensor
  - IMS15: IMS15-Module
  - SEISMIC: Seismic sensor
  - MAGNETIC: Magnetic sensor
  - SE: Switching interface
  - TA: Tableaus
  - HOLDUP: Holdup
  - VM: Showcase sensor
  - MANUAL: Manual detection
  - GENERIC: Generic detection
  - BOLT: Bolt sensor
    If no type is defined, DCC will use a standard icon for the graphic display
- @@N:x@@ Name information: If an input of a detector is labelled with this tag, the detector will accordingly receive the name provided.
- @@N:x@@ Name information: If an input of a detector is labelled with this tag, the detector will accordingly receive the name provided.

Example:
Input 1: @@ID:1@@N: Motion Detection Ost@@T:PIR@@
Input 2: @@ID:2@@N:Motion Detection West@@T:PIR@@
Input 3: @@ID:1@@
Input 4: @@ID:1@@
→ One Detector of type PIR with name „Motion Detection East“ with inputs 1, 3, 4
→ One Detector of type PIR with name „Motion Detection West“ with input 2

!	***PLEASE NOTE***
	Those detectors that are connected via an LSN-Gateway do not require additional configurations by means of the comment fields to further specify structural- and type information. The reason for this is, that this information will already be available by the interface. **However, if the comment fields are still filled, this information entered will have a higher priority.**

Hardware component types and their inputs

The hardware component types are based on static modelling and will be transferred via the SiInt-integration (referring to either the SiInt-unit type or the type-ID of the HW-module, if LSN-HW-modules are involved). The input types are pre-defined and assigned to in a distinct manner by the addressing procedure of the inputs.

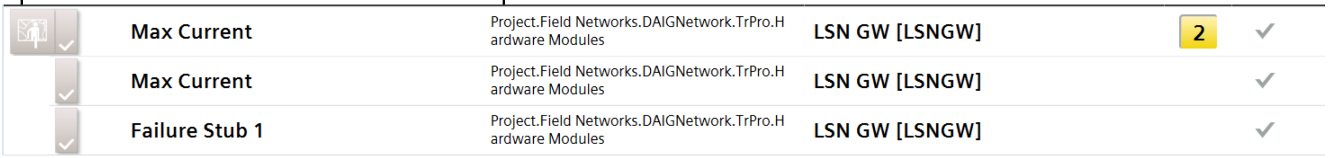
Example CPC:

- Type “Missing” at address-M
- Type “Open” at address-O
- Type “Threat” at Address-2
- Type “PIN-Code-Alarm” at address-3

These individual DCC alarms types will be generated for the hardware modules in accordance with the above-mentioned input addresses.

Example: The DCC-alarm -type “PIN-Code-Alarm” will occur, if a SiInt alarm for the input address-3 is being triggered.

As a hardware module can trigger several inputs at the same time, several DCC-alarms originating the same inputs can be active for one hardware component as well:



Max Current	Project.Field Networks.DAIGNetwork.TrPro.Hardware Modules	LSN GW [LSNGW]	2	✓
Max Current	Project.Field Networks.DAIGNetwork.TrPro.Hardware Modules	LSN GW [LSNGW]		✓
Failure Stub 1	Project.Field Networks.DAIGNetwork.TrPro.Hardware Modules	LSN GW [LSNGW]		✓

Detector types and alarms, which are (or can be) triggered by the detectors

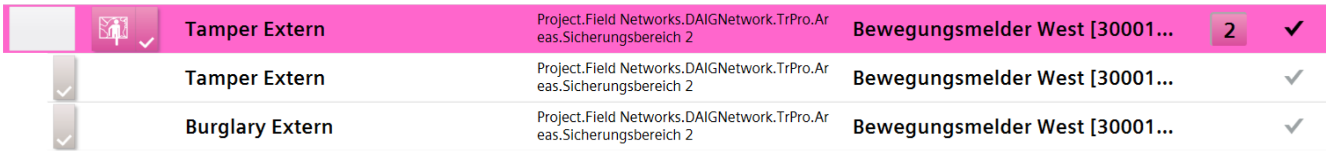
The alarm-types for the hardware modules must be modelled explicitly. In contrast however, for the detectors, different classes of types are defined:

- PIR: Motion detection
- FIRE: Fire detection
- GLASS: Glass break sensor
- IMS15: IMS15-Module
- SEISMIC: Seismic sensor
- MAGNETIC: Magnetic sensor
- SE: Switching interface
- SK: Schließblechkontakt
- HOLDUP: Holdup
- VM: Showcase sensor
- MANUAL: Manual detection
- GENERIC: Generic detection

SiInt determines the duration of the alarm types which are triggered by the detector. Therefore, these types have no impact on the status of the detector or its control and alarm behavior. These types are solely used for displaying different icons.

Those types of alarms, which can be triggered by a detector, originate from Siveillance Intrusion’s supported 33 types of alarms. For example, “info”, “warning “, “external intrusion”, “internal intrusion“, etc.

As a detector can trigger several inputs at the same time, several DCC-alarms originating from the corresponding alarm type can be active for one a detector as well:

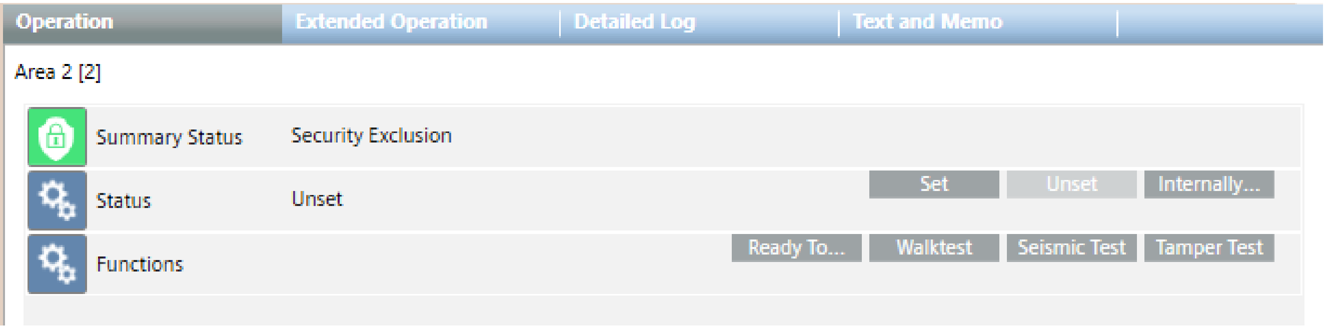


Tamper Extern	Project.Field Networks.DAIGNetwork.TrPro.Areas.Sicherungsbereich 2	Bewegungsmelder West [30001...	2	✓
Tamper Extern	Project.Field Networks.DAIGNetwork.TrPro.Areas.Sicherungsbereich 2	Bewegungsmelder West [30001...		✓
Burglary Extern	Project.Field Networks.DAIGNetwork.TrPro.Areas.Sicherungsbereich 2	Bewegungsmelder West [30001...		✓

4.2.2 Status/States and Control of Areas, Hardware Components and Detectors

4.2.2.1 Areas

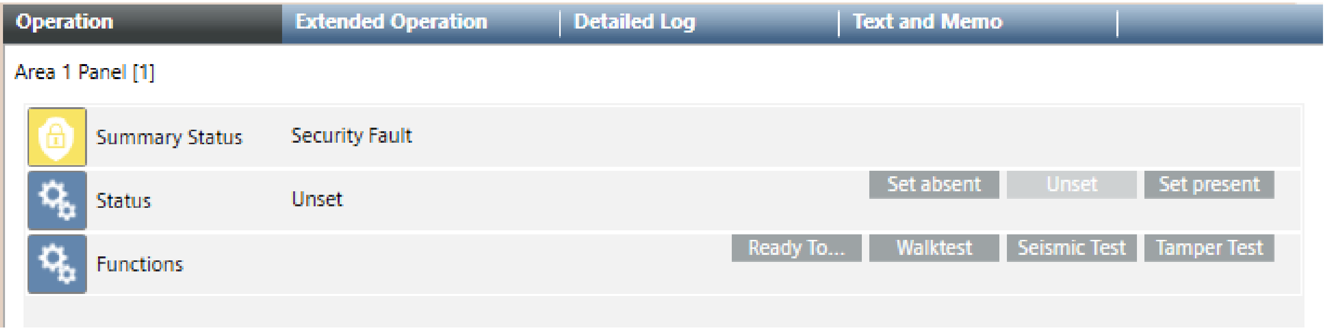
An area state is displayed in accordance with the same state information received by SiInt. The ability to control a state depends on the area type.



Area 2 [2]

Summary Status	Security Exclusion
Status	Unset
Functions	

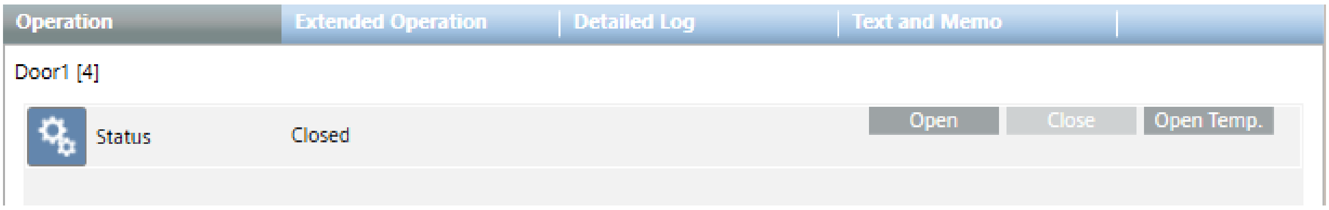
State/Status & Control of an Intrusion Area



Area 1 Panel [1]

Summary Status	Security Fault
Status	Unset
Functions	

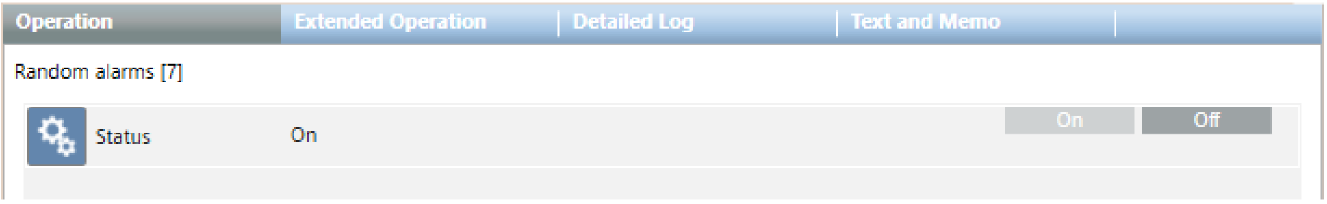
State/Status & Control of a Present/Absent Area



Door1 [4]

Status	Closed

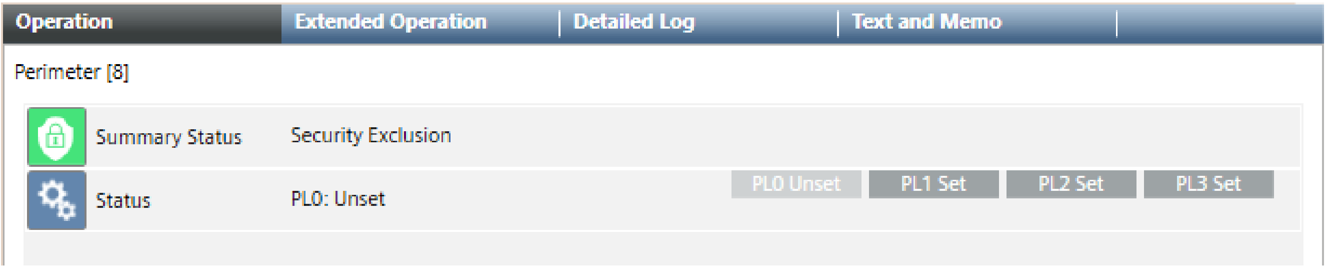
State/Status & Control of Doors



Random alarms [7]

Status	On

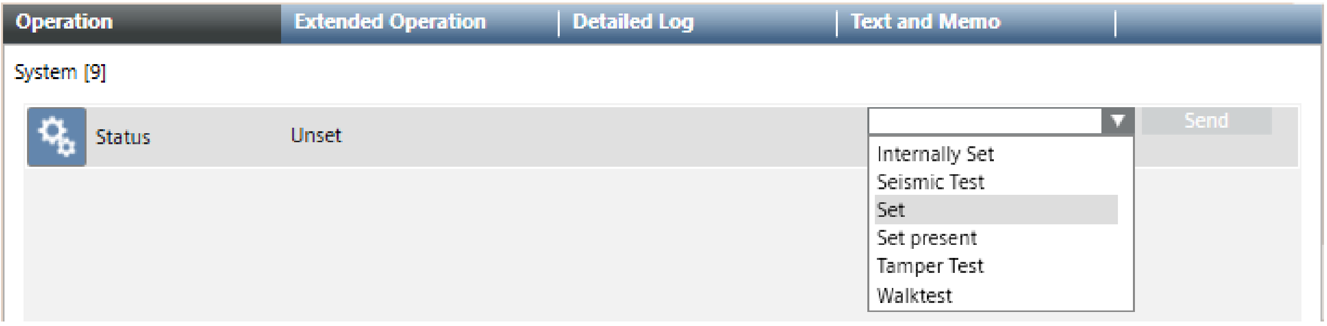
State/Status & Control of On-/Off-Areas



Perimeter [8]

Summary Status	Security Exclusion
Status	PL0: Unset

State/Status & Control of Perimeter Areas



System [9]

Status Unset

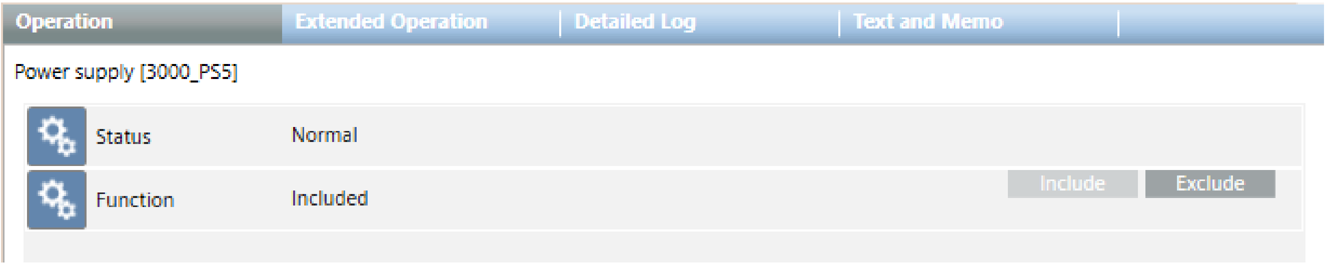
State/Status & Control of Generic Areas

4.2.2.2 Hardware Components

Hardware components aggregate multiple inputs. Therefore, the status of a hardware component is an aggregated one, displaying the alarm type of the most critical triggering input.

For example, if a PS5 “open’-input and “power failure”-input are triggered simultaneously, the intrusion will be considered as more critical, and the aggregated state of “holdup” will be received.

The property “mode” allows a hardware component to be either switched on or off. This control option is applicable to all inputs of the respective hardware component involved.



Power supply [3000_PS5]

Status Normal

Function Included

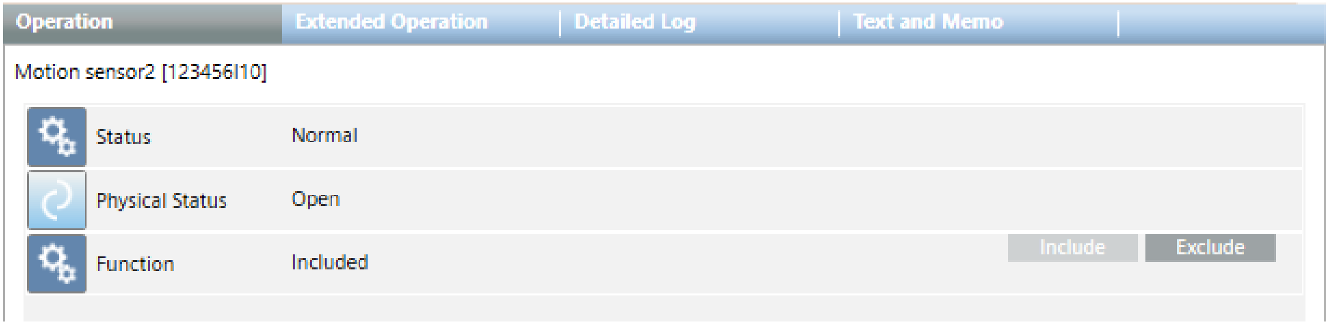
Aggregated Status/State and Control of a Hardware Component

4.2.2.3 Detectors

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

The physical state aggregates the physical condition of the detector’s inputs (closed, open, etc.) to an aggregated state, which considers for example “sabotage” more critical than “open”.

The property “mode” allows a detector to be either switched on or off. This control option is applicable to all inputs of the respective detector involved.



Motion sensor2 [123456I10]

Status Normal

Physical Status Open

Function Included

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

4.2.3 Alarms / Warnings of Areas, Hardware Components and Detectors

The SiInt-integration includes the use of both DCC-management-station-alarms and field-system-alarms:

4.2.3.1 SiInt-Device

- Connection monitoring (Management Station-Alarm, Fault_NoReset)
- Driver monitoring (Management Station-Alarm, Fault_NoReset)
- Notification of configurational changes (Management Station-Alarm, Fault_NoReset)
- License warning (Management Station-Alarm, Fault_NoAckReset)

4.2.3.2 Intrusion Area

Unsetting an area (Management Station-Alarm, ArmDisarm_NoAckNoReset)

4.2.3.3 Hardware Component

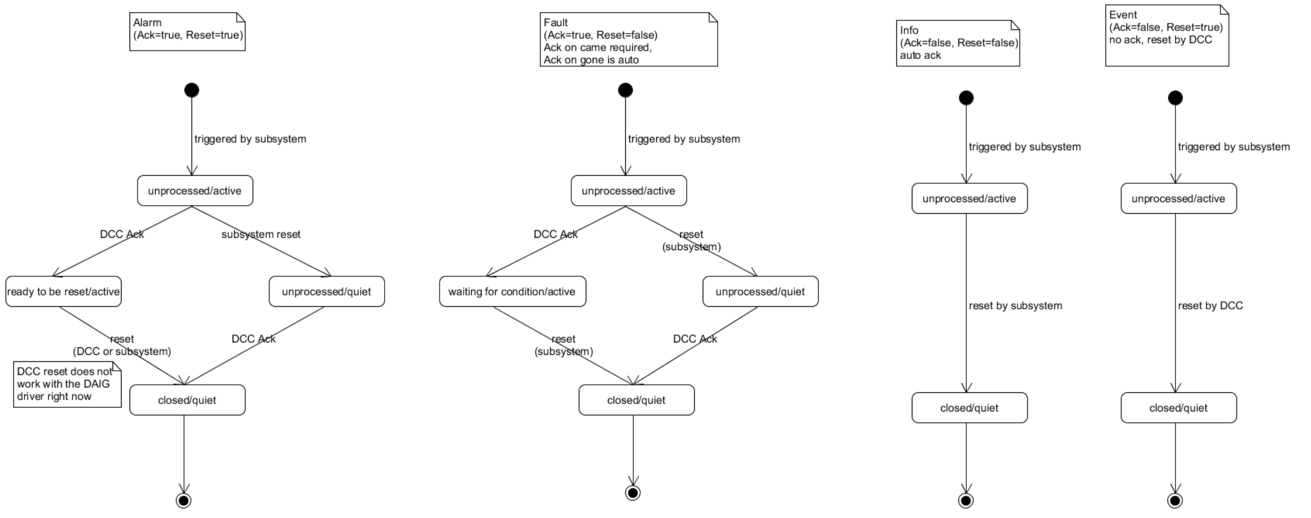
Triggered input (SiInt-Alarm), Field System-Alarm, standard behavior via the default-alarm table (please refer to section 4.2.3.5)

4.2.3.4 Detector

Triggered input (SiInt-alarm), Field system-alarm, standard behavior via the default-alarm table (please refer to section 4.2.3.5)

4.2.3.5 Alarm-State Diagrams for Field System-Alarms

Depending on the category for either the alarm type (detector) or the input type (hardware component), the alarm-reset (“Reset”) or alarm-acknowledgement (“Ack”) behavior is defined differently in the standard-DCC-alarm-table:



4.3 Access to SiInt

The SiInt connection to DCC allows access to configurational and operational data. This is enabled by the SSH-interface of the SiInt-system.

For this purpose, during the installation process, the SSH-certificates must be exchanged between SiInt and DCC (the DCC-driver). In addition, the SSH-user of the SiInt-system must be configured accordingly authorizing him/her to access the configurational and operational data (please see below).

Please note, that this configured SSH-user will be the only one, who is authorized and able to access the SiInt-system. Therefore his/her user rights must be limited and administered accordingly via DCC (defining which DCC-user can access which areas, detectors, etc.).

The comment field information of the inputs is used to enhance the configurational data with structural information (please refer to section 4.2.1.2). This will be supported from the SiInt-version V8 onwards.

4.4 Licensing

The following will describe the licensing procedure for the SiInt-connection:

The SiInt-license will require as a basis the SiInt-license. Please refer to section 4.4.1.2 for pricing, order numbers and further information.

4.4.1.1 Security-Datapoints

Please see below a listing of security/SCADA – datapoints, which are required for the use of the SiInt-interface via DCC:

- DAIG-driver = 0 Datapoints
- DAIG-network = 0 Datapoints
- Siv. Intrusion-device = 0 Datapoints
- Intrusion Area = 0 Datapoints
- Present/Absent Areas = 0 Datapoints
- Door = 1 Security-Datapoint
- On-/Off-Area = 1 Security-Datapoint
- Perimeter Areas = 0 Datapoints
- Hardware Component = 0 Datapoints
- Detector = 1 Security-Datapoint
- Manual Area = 1 Security-Datapoint

Only the imported objects will require datapoints.

4.4.1.2 Licensing the DAIG-Interface

To integrate Siveillance Intrusion PRO/ADV into Desigo CC, the following one-time license named “Intrusion PRO/ADV Integration into DCC“ is required.

For Panels with less than 400 detectors, you can use the Intrusion DCC Integration (Entry)-License. If the panel is bigger than 400 detectors you have to use the standard Intrusion in DCC-License or a combination of Intrusion DCC (Entry)- License and Intrusion DCC Integration (Upsell)-License.

For usage of the redundancy function, you must provide 2 licenses of the same level (e.g. 2x Entry License oder 2x Standard License).

Modul	SSN	Anzahl
Intrusion DCC Integration	P54594-P416-A100-D	1
Intrusion DCC Integration (Entry)	P54594-P416-A101-D	1
Intrusion DCC Integration (Upsell)	P54594-P416-A102-D	1

Please refer to the PLN/SDR (Sales and Delivery Release Note) for further details related to licensing & pricing.

5 Configuration of SSH-Access to Siveillance Intrusion PRO/ADV (SiInt)

5.1 SiInt System Requirements

The pre-condition to use the SiInt-integration to DCC is the existence of a MP2.0 SiInt PRO/ADV system (starting at the NOX-firmware version 10.51p) or higher.

!	***PLEASE NOTE***
	The connection to the SiInt-system is cancelled generating a corresponding note, if the SiInt-integration detects a SiInt-system-version, which is lower than 10.51p.

5.2 Encrypted communication with Sint PRO/ADV

The encrypted communication from the DAIG-04—Driver to the SiInt system is performed via SSH / public key authentication exchanging the individual public keys of the client computer (DCC computer) and the server (SiInt). This exchange takes place during the installation/commissioning phase. It ensures the following facts, which are essential for operational efficiency:

- DCC will communicate with the correct SiInt PRO/ADV system
- Only the DCC client computer in use is authorized to register via this certificate and via SSH with the corresponding SiInt PRO/ADV system.

Thus, so called *man-in-the-middle-attacks* are excluded.

The following method is recommended for this configuration:

1. Create a pair of SSH-keys for the Desigo CC computer
2. Save the private Desigo CC-key in the DCC project directory
3. Create a pair of SSH-keys for the SiInt-system (if not yet available)
4. Store the private SiInt-key in the configurational tool of SiInt
5. Store the public DCC-key from with the SiInt-SSH-user
6. Keep/save the public SiInt-key

To generate SSH-keys, please refer to free tools like **Putty** or **Puttygen.** Both can be downloaded for free at www.putty.org.

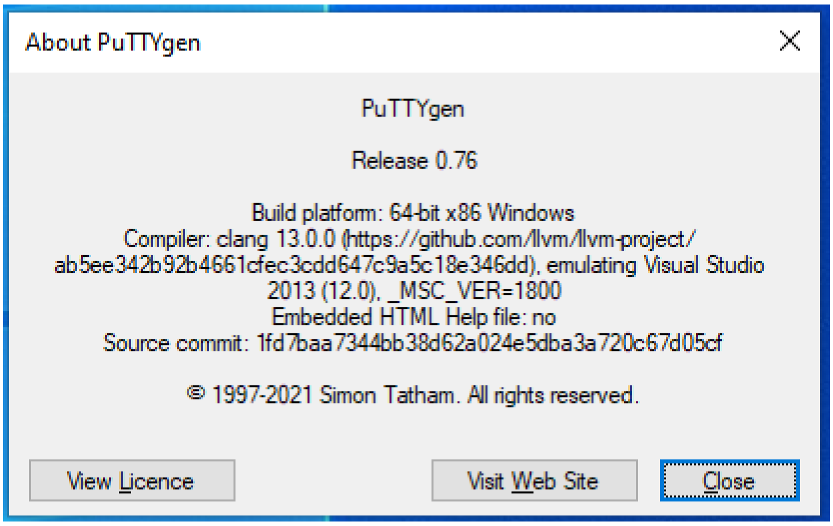
!	***PLEASE NOTE***
	To grant access to the SiInt-SSH-Port, Port 22 must be enabled as an outgoing port within the Windows-firewall of Desigo CC. Also, please refer to the DCC Installation Manual / Configuring Windows Firewall Settings.

5.2.1 Create a pair of SSH-keys for Desigo CC using the support of Puttygen

!

PLEASE NOTE

If you are using a later version of puttygen than 0.74, you have to set the PPK file version to 2 before generating the keys. Siveillance Intrusion Pro does not work with key version 3.
The version of puttygen can be found in the options „Help“ → „About“:



About PuTTYgen

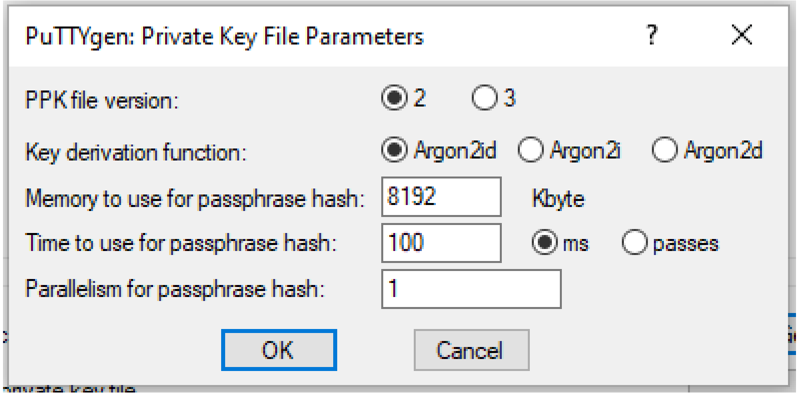
PuTTYgen

Release 0.76

Build platform: 64-bit x86 Windows
Compiler: clang 13.0.0 (https://github.com/llvm/llvm-project/ ab5ee342b92b4661cfec3cdd647c9a5c18e346dd), emulating Visual Studio 2013 (12.0), _MSC_VER=1800
Embedded HTML Help file: no
Source commit: 1fd7baa7344bb38d62a024e5dba3a720c67d05cf

© 1997-2021 Simon Tatham. All rights reserved.

To change the PPK file version to 2, navigate to „Key“ → „Parameters for Key saving files…“:



PuTTYgen: Private Key File Parameters

PPK file version: ● 2 ○ 3

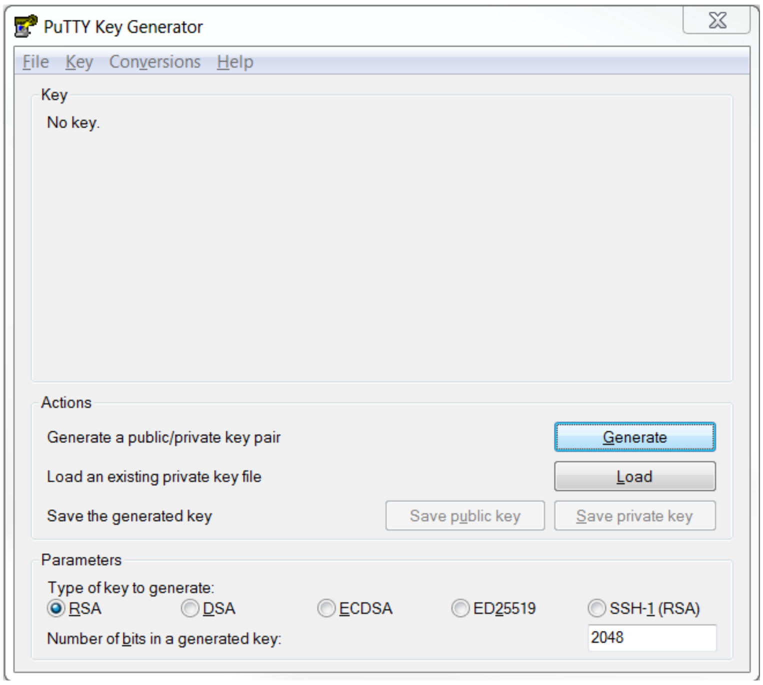
Key derivation function: ● Argon2id ○ Argon2i ○ Argon2d

Memory to use for passphrase hash: 8192 Kbyte

Time to use for passphrase hash: 100 ● ms ○ passes

Parallelism for passphrase hash: 1

After starting Puttygen, the interface shown below will be displayed. **Please note the following: Key type “RSA” including a bit length of 2048 must be selected.** To generate a key, please confirm with “Generate”.



No key.

Generate a public/private key pair

Load an existing private key file

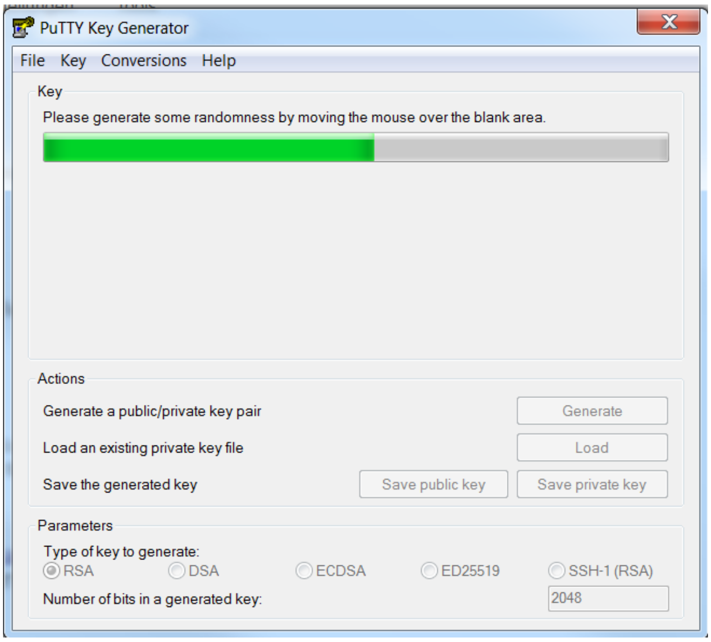
Save the generated key

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Figure 2: Puttygen Key Generator Window

Move the cursor inside the upper empty area of the Puttygen Key Generator to create the pair of keys. The green bar represents the current progress.



Please generate some randomness by moving the mouse over the blank area.

Generate a public/private key pair

Load an existing private key file

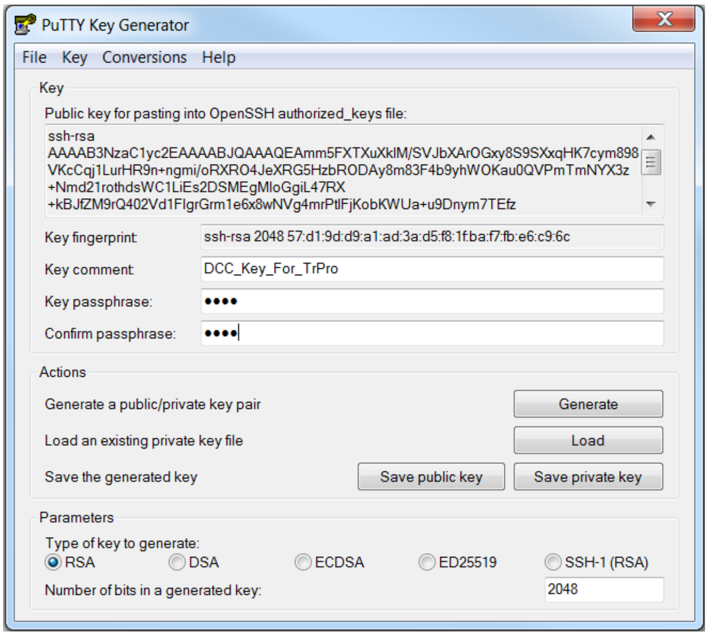
Save the generated key

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Figure 3: Generating a Key

Once the process for generating a key is completed, the “Key comment” can be adjusted in the next window (example name: “DCC_Key_For_TrPro”). Afterwards a password to access the private key file must be set. This password must later be entered into the connection-configuration of the SiInt-integration within Desigo CC.



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAmm5FXTXuXklM/SVJbXArOGxy8S9SXxqHK7cym898
VKcCqj1LurHR9n+ngmi/oRXRO4JeXRG5HzbRODAy8m83F4b9yhWOKau0QVPmTmNYX3z
+Nmd21rothdsWC1LiEs2DSMEgMloGgiL47RX
+kBJfZM9rQ402Vd1FlgrGrm1e6x8wNVg4mrPtlFjKobKWUa+u9Dnym7TEfz
```

Key fingerprint: ssh-rsa 2048 57:d1:9d:d9:a1:ad:3a:d5:f8:1f:ba:f7:fb:e6:c9:6c

Key comment: DCC_Key_For_TrPro

Key passphrase: ••••

Confirm passphrase: ••••

Generate a public/private key pair

Load an existing private key file

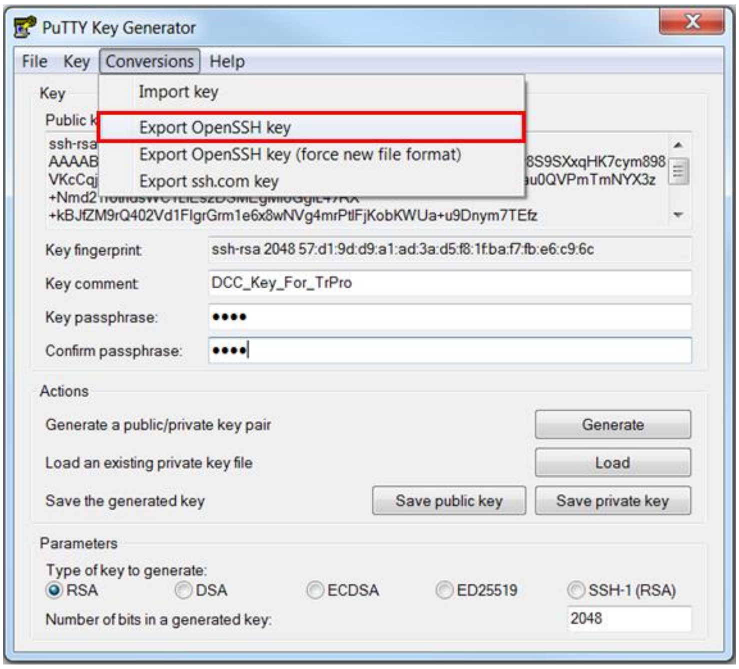
Save the generated key

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Figure 4: Describing the Key

This key must be saved in the “OpenSSH” format. Please move the tab **“Conversions”** and select the option **“Export OpenSSH key”.**



Key fingerprint: ssh-rsa 2048 57:d1:9d:d9:a1:ad:3a:d5:f8:1f:ba:f7:fb:e6:c9:6c

Key comment: DCC_Key_For_TrPro

Key passphrase: ••••

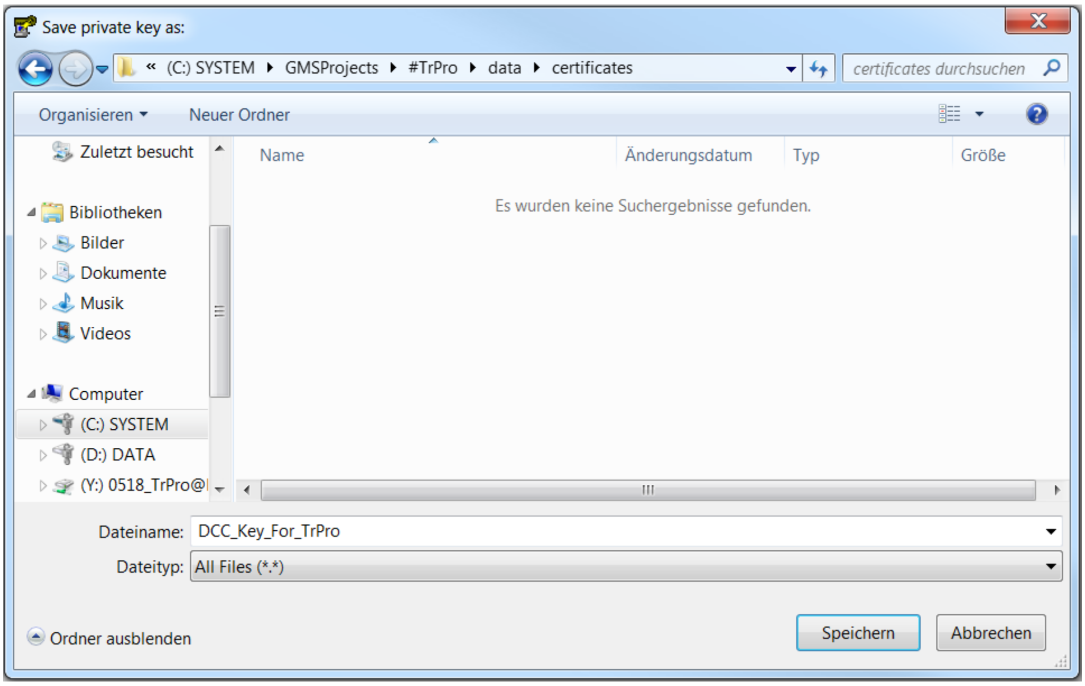
Confirm passphrase: ••••

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Figure 5: Saving the Key

A dialogue box will open. Here the file location for the private key which is to be exported can be selected. For this purpose, please generate a folder named „**certificates**“ in the following directory-location: **„../GMSProjects/<ProjectName>/data/“**. This certificate file must later be entered into the connection configuration of the SiInt-interface within Desgo CC.



Save private key as:

« (C:) SYSTEM ▸ GMSProjects ▸ #TrPro ▸ data ▸ certificates

Es wurden keine Suchergebnisse gefunden.

Dateiname: DCC_Key_For_TrPro

Dateityp: All Files (*.*)

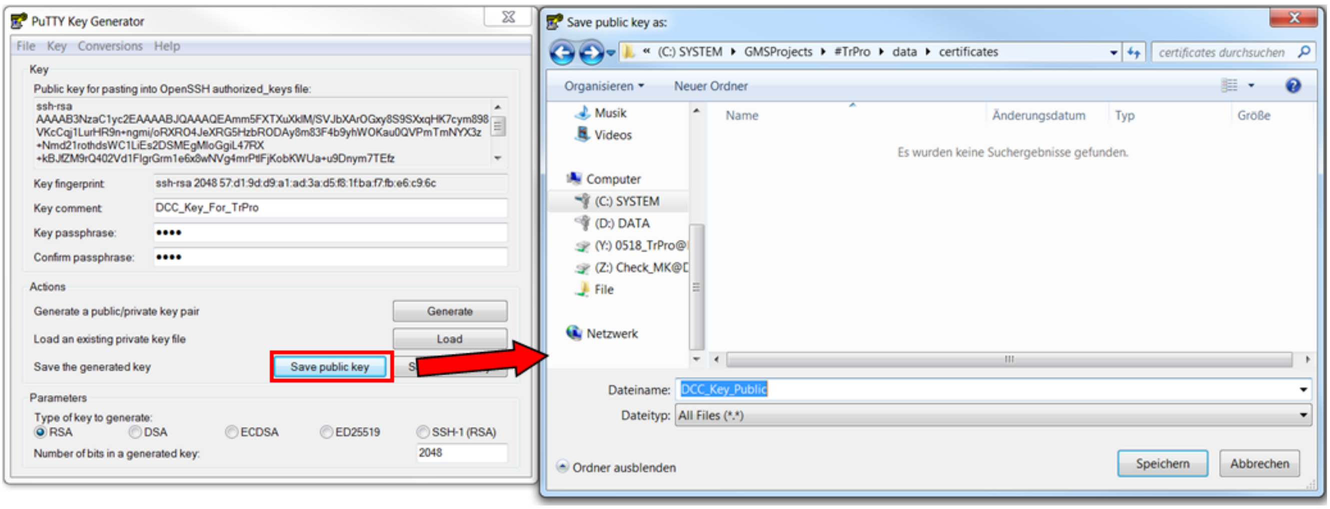
Figure 6: Saving the Key, Selecting Folders

!	*PLEASE NOTE*
	Please save the certificates in the folder or in a sub-folder of the "data" project directory assuring that these will also be saved in the event of a backup.

Do not close Puttygen yet, as it will be required for the next step still.

5.2.2 Save the public key for DCC

The public part of the key must be saved separately, as this key information must be later entered into SiInt. For this purpose, please use the option "Save public key".



PuTTY Key Generator

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAmm5FXTXuXkIM/SVJbXArOGxy8S9SXxqHK7cym898
VKcCqj1LurHR9n+ngmi/oRXRO4JeXRG5HzbRODAy8m83F4b9yhWOKau0QVPmTmNYX3z
+Nmd21rothdsWC1LiEs2DSMEgMloGgiL47RX
+kBJfZM9rQ402Vd1FlgrGrm1e6x8wNVg4mrPtlFjKobKWUa+u9Dnym7TEfz
```

Key fingerprint: ssh-rsa 2048 57:d1:9d:d9:a1:ad:3a:d5:f8:1f:ba:f7:fb:e6:c9:6c

Key comment: DCC_Key_For_TrPro

Key passphrase: ••••

Confirm passphrase: ••••

Type of key to generate: ● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Save public key as:

« (C:) SYSTEM ▸ GMSProjects ▸ #TrPro ▸ data ▸ certificates

Es wurden keine Suchergebnisse gefunden.

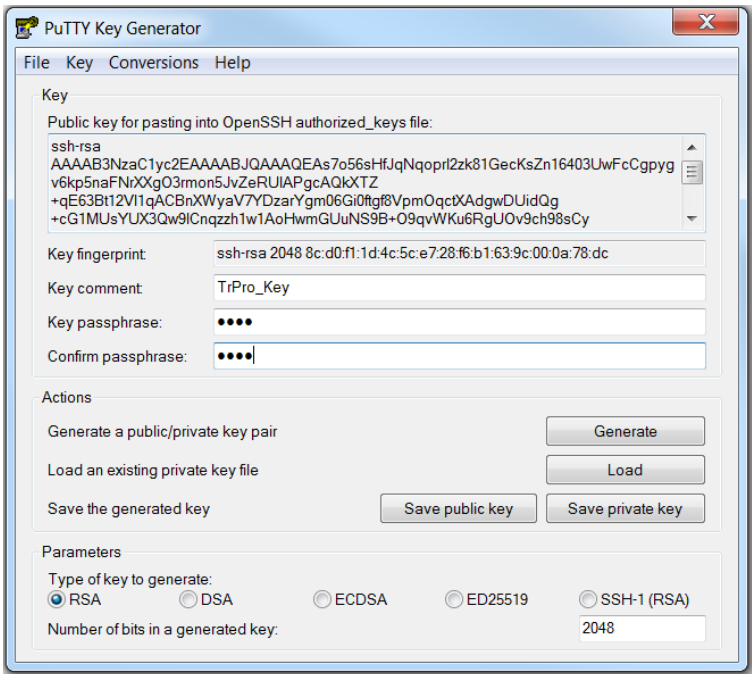
Dateiname: DCC_Key_Public

Dateityp: All Files (*.*)

Figure 7: Saving the public DCC key

5.2.3 Create a pair of keys for Siveillance Intrusion PRO/ADV

If no key was entered into the SSH settings of SiInt, a second key must be generated. For this purpose, please generate once again a key via Puttygen.



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAs7o56sHfJqNqoprl2zk81GecKsZn16403UwFcCgpyg
v6kp5naFNrXXgO3rmon5JvZeRUlAPgcAQkXTZ
+qE63Bt12Vl1qACBnXWyaV7YDzarYgm06Gi0ftgf8VpmOqctXAdgwDUidQg
+cG1MUsYUX3Qw9lCnqzzh1w1AoHwmGUuNS9B+O9qvWKu6RgUOv9ch98sCy
```

Key fingerprint: ssh-rsa 2048 8c:d0:f1:1d:4c:5c:e7:28:f6:b1:63:9c:00:0a:78:dc

Key comment: TrPro_Key

Key passphrase: ••••

Confirm passphrase: ••••

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

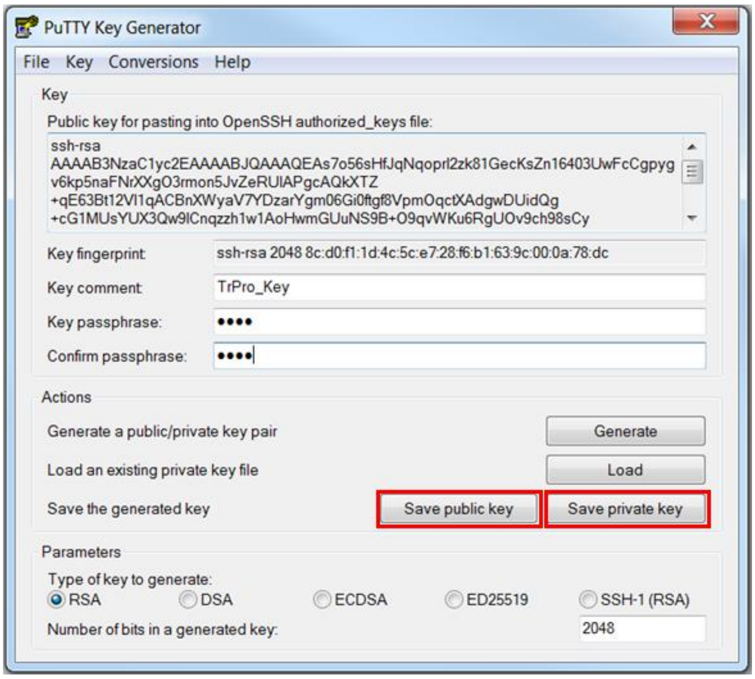
Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Figure 8: SiInt-Key

For this key both a private and a public key each must be saved. Please use the options “Save public key” and “Save private key”.



PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAs7o56sHfJqNqoprl2zk81GecKsZn16403UwFcCgpyg
v6kp5naFNrXXgO3rmon5JvZeRUlAPgcAQkXTZ
+qE63Bt12Vl1qACBnXWyaV7YDzarYgm06Gi0ftgf8VpmOqctXAdgwDUidQg
+cG1MUsYUX3Qw9lCnqzzh1w1AoHwmGUuNS9B+O9qvWKu6RgUOv9ch98sCy

Key fingerprint: ssh-rsa 2048 8c:d0:f1:1d:4c:5c:e7:28:f6:b1:63:9c:00:0a:78:dc

Key comment: TrPro_Key

Key passphrase: ••••

Confirm passphrase: ••••

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key Save private key

Parameters

Type of key to generate:

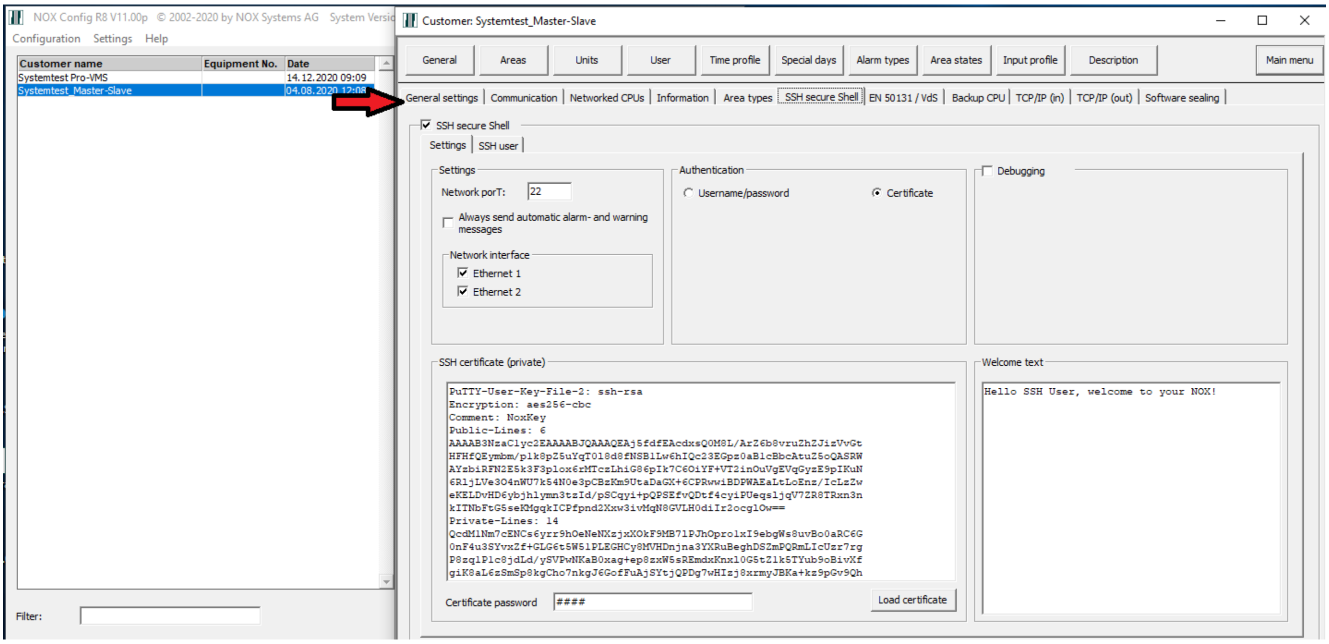
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Figure 9: Saving the key for Siveillance Intrusion

5.2.4 Registering a Key in Siveillance Intrusion

For registering a private SiInt-key in the SiInt-system, the SiInt-Config-Tool (NOX Config) is required. The corresponding configuration needed must be selected via this tool.



Customer name	Equipment No.	Date
Systemtest Pro-VMS		14.12.2020 09:09
Systemtest_Master-Slave		04.08.2020 12:08

☑ SSH secure Shell

Settings

Network porT: 22

□ Always send automatic alarm- and warning messages

Network interface

☑ Ethernet 1

☑ Ethernet 2

Authentication

○ Username/password ● Certificate

□ Debugging

SSH certificate (private)

```
PuTTY-User-Key-File-2: ssh-rsa
Encryption: aes256-cbc
Comment: NoxKey
Public-Lines: 6
AAAAB3NzaC1yc2EAAAABJQAAAQEAj5fdfEAcdxsQ0M8L/ArZ6b8vruZhZJizVvGt
HFHfQEymbm/p1k8pZ5uYqT0l8d8fNSB1Lw6hIQc23EGpz0aB1cBbcAtuZ5oQASRW
AYzbiRFN2E5k3F3plox6rMTczLhiG86pIk7C6OiYF+VT2inOuVgEVqGyzE9pIKuN
6RljLVe3O4nWU7k54N0e3pCBzKm9UtaDaGX+6CPRwwiBDPWAEaLtLoEnz/IcLzZw
eKELDvHD6ybjhlymn3tzId/pSCqyi+pQPSEfvQDtf4cyiPUeqsljqV7ZR8TRxn3n
kITNbFtG5seKMgqkICPfpnd2Xxw3ivMqN8GVLH0diIr2ocglOw==
Private-Lines: 14
QcdM1Nm7cENCs6yrr9hOeNeNXzjxXOkF9MB71PJhOprolxI9ebgWs8uvBo0aRC6G
0nF4u3SYvxZf+GLG6t5W51PLEGHCy8MVHDnjna3YXRuBeghDSZmPQRmLIcUzr7rg
P8zq1P1c8jdLd/ySVPwNKaB0xag+ep8zxW5sREmdxKnxl0G5tZ1k5TYub9oBivXf
giK8aL6zSmSp8kgCho7nkgJ6GofFuAjSYtjQPDg7wHIzj8xrmyJBKa+kz9pGv9Qh
```

Certificate password ####

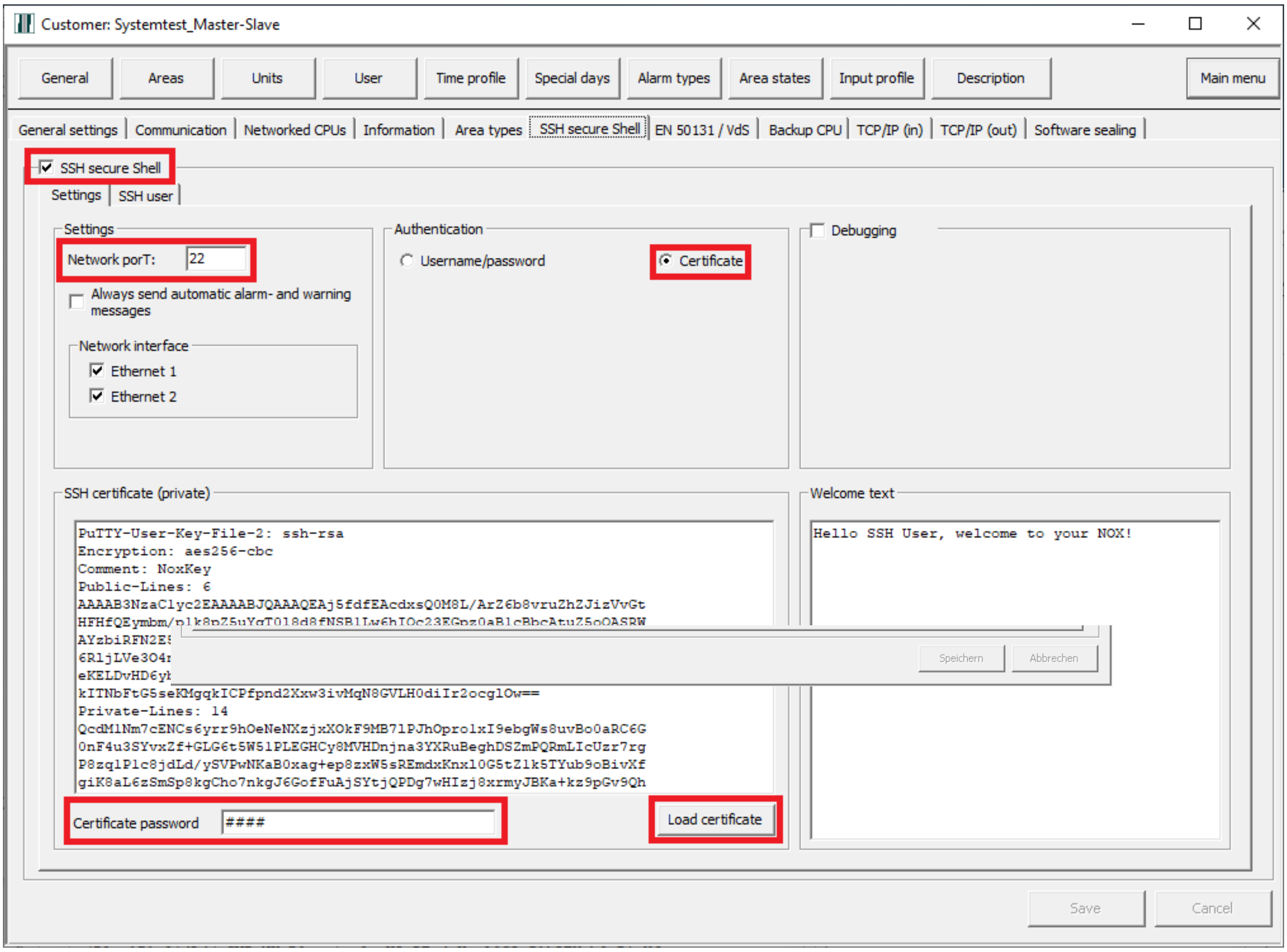
Welcome text

```
Hello SSH User, welcome to your NOX!
```

Figure 10: SiInt-Config-Tool including the opening of the configuration

Please select the “SSH Secure Shell” tab and follow these configurational steps:

1. Check the box “SSH Secure Shell”
2. Configure the port (standard: 22)
3. Select “Certificate” in the Authentication area
4. Confirm the button “Load Certificate” and select the configuration file (private configuration file for Siveillance Intrusion created in the previous step)
5. Enter the password of the configuration file
6. Press the save button (on the bottom right)



☑ SSH secure Shell

Settings

Network porT: 22

□ Always send automatic alarm- and warning messages

Network interface

☑ Ethernet 1

☑ Ethernet 2

Authentication

○ Username/password ● Certificate

□ Debugging

SSH certificate (private)

```
PuTTY-User-Key-File-2: ssh-rsa
Encryption: aes256-cbc
Comment: NoxKey
Public-Lines: 6
AAAAB3NzaC1yc2EAAAABJQAAAQEAj5fdfEAcdxsQ0M8L/ArZ6b8vruZhZJizVvGt
HFHfQEymbm/p1k8pZ5uYqT018d8fNSB1Lw6hIOc23EGpz0aB1cBbcAtuZ5oOASRW
AYzbiRFN2E5
6R1jLVe3O4r
eKELDvHD6yk
kITNbFtG5seKMgqkICPfpnd2Xxw3ivMqN8GVLH0diIr2ocglOw==
Private-Lines: 14
QcdM1Nm7cENCs6yrr9hOeNeNXzjxXOkF9MB71PJhOpro1xI9ebgWs8uvBo0aRC6G
0nF4u3SYvxZf+GLG6t5W51PLEGHCy8MVHDnjna3YXRuBeghDSZmPQRmLIcUzr7rg
P8zq1P1c8jdLd/ySVPwNKaB0xag+ep8zxW5sREmdxKnx10G5tZ1k5TYub9oBivXf
giK8aL6zSmSp8kgCho7nkgJ6GofFuAjSYtjQPDg7wHIzj8xrmyJBKa+kz9pGv9Qh
```

Certificate password: ####

Load certificate

Welcome text

```
Hello SSH User, welcome to your NOX!
```

Figure 11: Configuration of the SSH interface in SiInt

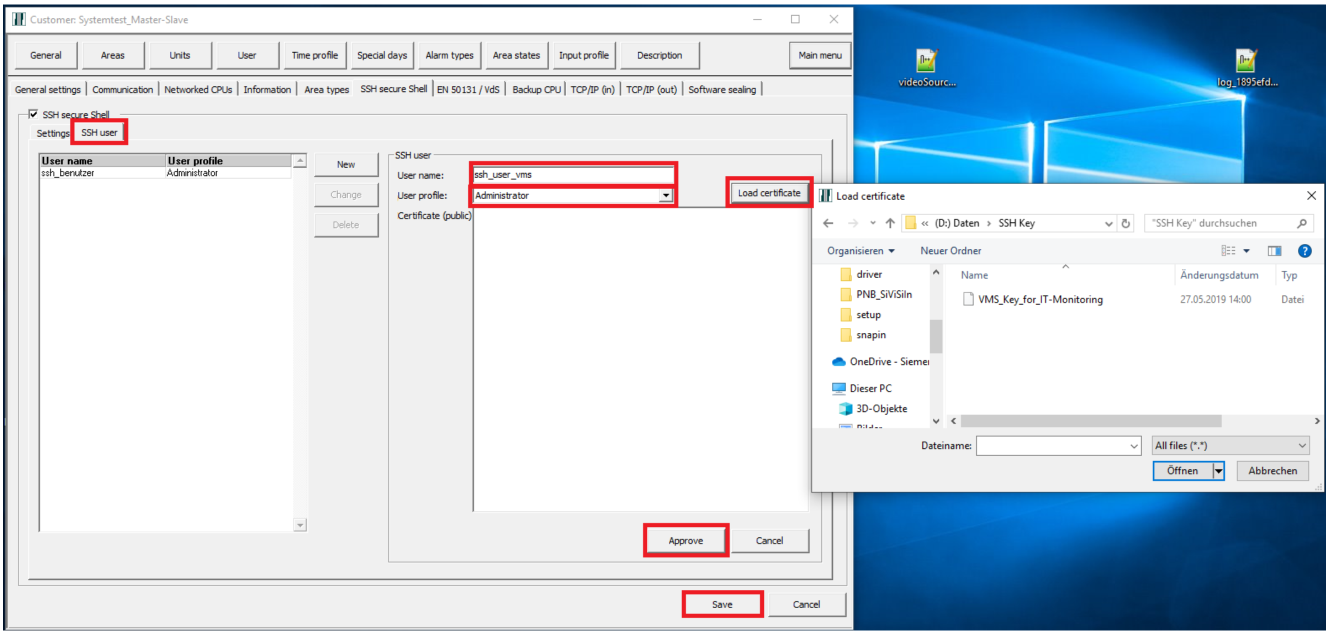
!	***PLEASE NOTE***
	A warning message stating that all saved passwords will be deleted, will appear, if one or more SSH users were already created and if the authentication of “username/password” is now switched to „certificate “. **This dialogue box can be confirmed with “Yes”, as this message only applies to the SSH-passwords and not to the passwords of the Siveillance Intrusion PRO/ADV users.**

5.2.5 Configure SiInt-users for SSH access

A SiInt-SSH-user must be created to enable the communication of DCC with the SiInt-system. This SSH-user must apply the public key of the DCC computer.

For this purpose, please switch to the “SSH User” tab within the SiInt-configuration. Please follow these steps to create a new user:

1. Select the button „New“
2. Enter a username
3. Assign a user profile
4. Select “Load Certificate” and select the public key from the DCC-computer („Dcc_Key_Public“)
5. Select “Approve”
6. Select “Save”



User name	User profile
ssh_benutzer	Administrator

User name: ssh_user_vms

User profile: Administrator

Name	Änderungsdatum	Typ
VMS_Key_for_IT-Monitoring	27.05.2019 14:00	Datei

!	***PLEASE NOTE***
	The SSH-user name can appear in the warning message. This for example is the case in the event of deactivations. There it is highly recommended to use meaningful and self-explanatory names.

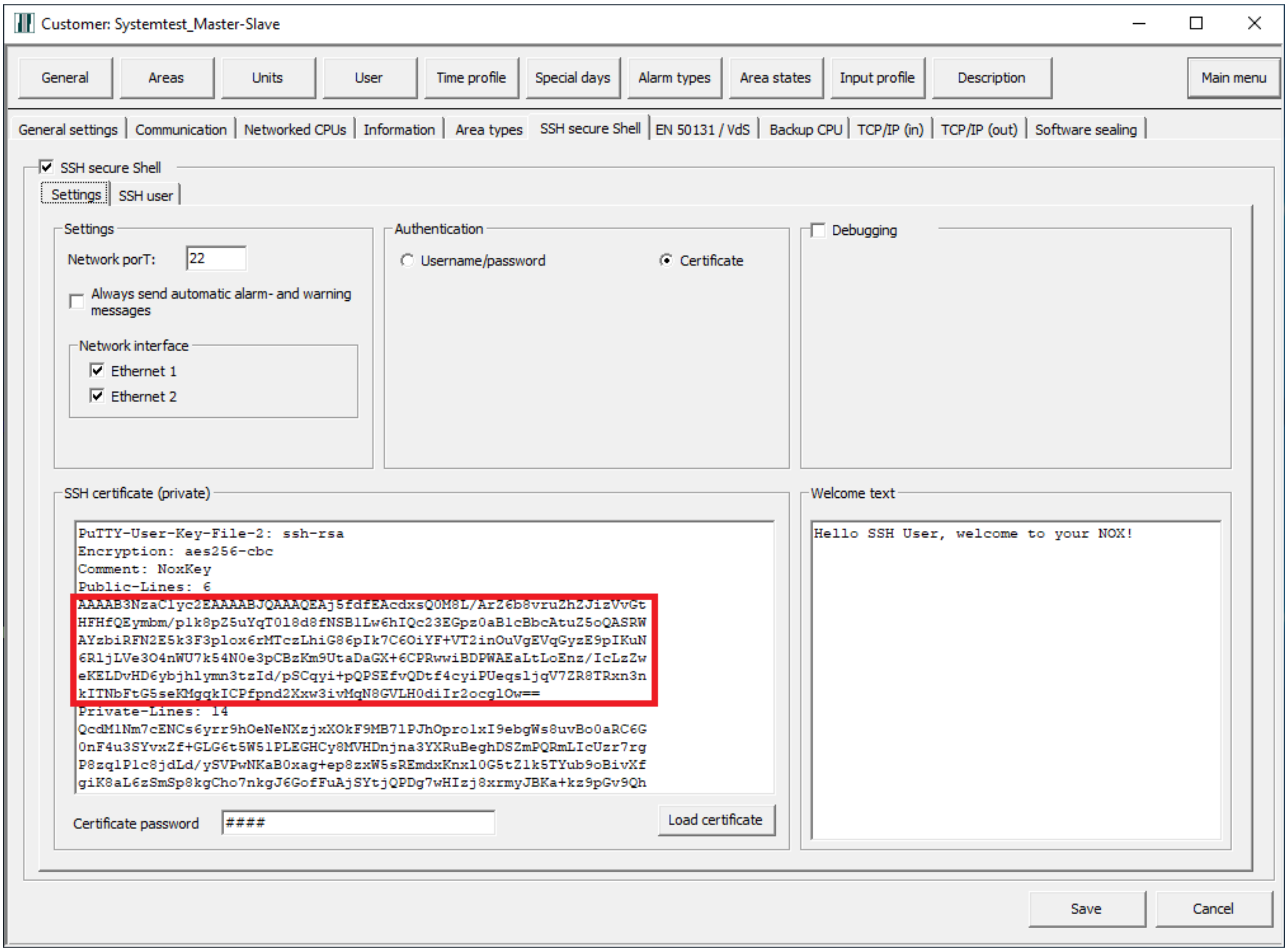
!	***PLEASE NOTE***
	Access to the SiInt-integration is facilitated by granting adequate authorizations to the SiInt-system user, who is assigned SSH-access as well. **Please ensure that this SiInt-system user has all authorizations required for technical operation. The SiInt-system includes one default profile named “Managementsystem”, which in general can be used to facilitate access to DCC.** **However, it is essential to ensure, that the user being used does not have too many rights preventing certain actions, such as unsetting an area via DCC which is secured by a block lock door.** **Within DCC, these “maximum” rights can be restricted via DCC-authorizations, that can be assigned specifically to various groups of users.** **Thus, for example only those users can set an area, who have the authorization “Extended”.**

!	***PLEASE NOTE***
	SSH user authorizations for VdS-compatible systems must be configured in the Intrusion-system side accordingly assuring that the interface complies with the VdS-required restrictions.

!	***PLEASE NOTE***
	For privacy reasons, please do not use personal data to define the name of the SSH user!

5.2.6 Read the Public Key from the SiInt-System

If the SiInt-certificate does not provide a public key file, the public key may also be copied from the SSH settings within the SiInt-Config Tool (NOX Config).



☑ SSH secure Shell

Settings

Network porT: 22

□ Always send automatic alarm- and warning messages

Network interface

☑ Ethernet 1

☑ Ethernet 2

Authentication

○ Username/password ● Certificate

□ Debugging

SSH certificate (private)

```
PuTTY-User-Key-File-2: ssh-rsa
Encryption: aes256-cbc
Comment: NoxKey
Public-Lines: 6
AAAAB3NzaC1yc2EAAAABJQAAAQEAj5fdfEAcdxsQ0M8L/ArZ6b8vruZhZJizVvGt
HFHfQEymbm/p1k8pZ5uYqT018d8fNSB1Lw6hIQc23EGpz0aB1cBbcAtuZ5oQASRW
AYzbiRFN2E5k3F3plox6rMTczLhiG86pIk7C6OiYF+VT2inOuVgEVqGyzE9pIKuN
6RljLVe3O4nWU7k54N0e3pCBzKm9UtaDaGX+6CPRwwiBDPWAEaLtLoEnz/IcLzZw
eKELDvHD6ybjhlymn3tzId/pSCqyi+pQPSEfvQDtf4cyiPUeqsljqV7ZR8TRxn3n
kITNbFtG5seKMgqkICPfpnd2Xxw3ivMqN8GVLH0diIr2ocglOw==
Private-Lines: 14
QcdM1Nm7cENCs6yrr9hOeNeNXzjxXOkF9MB71PJhOprolxI9ebgWs8uvBo0aRC6G
0nF4u3SYvxZf+GLG6t5W51PLEGHCy8MVHDnjna3YXRuBeghDSZmPQRmLIcUzr7rg
P8zqlPlc8jdLd/ySVPwNKaB0xag+ep8zxW5sREmdxKnxl0G5tZ1k5TYub9oBivXf
giK8aL6zSmSp8kgCho7nkgJ6GofFuAjSYtjQPDg7wHIzj8xrmyJBKa+kz9pGv9Qh
```

Certificate password ####

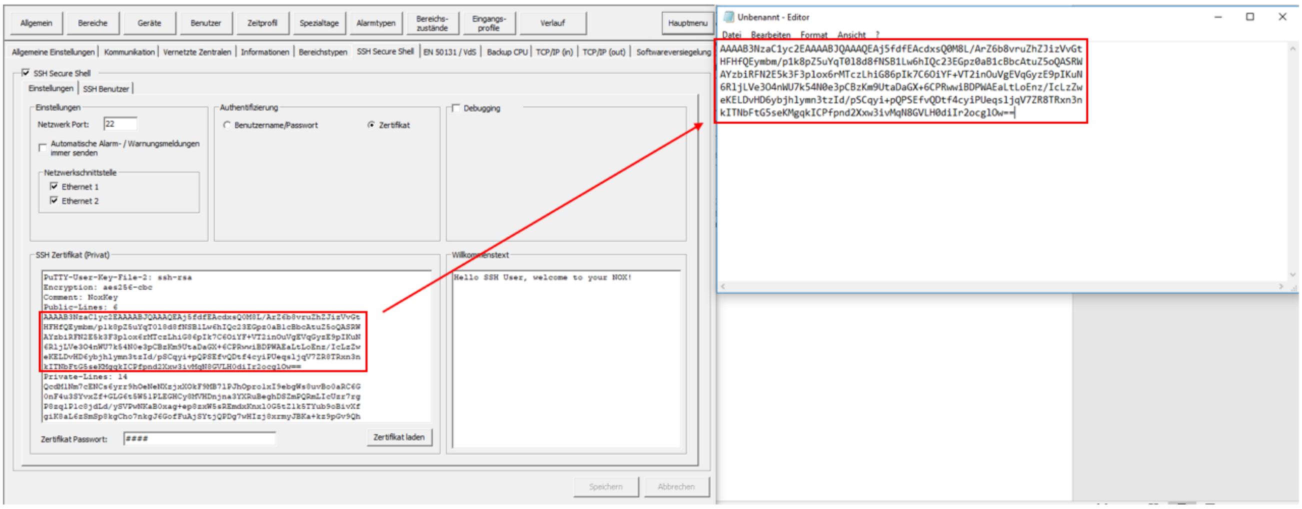
Welcome text

```
Hello SSH User, welcome to your NOX!
```

Figure 12: Public key of the SiInt-system

Depending on the format of the certificate used, the public key of the SiInt-system can be copied from “SSH Secure Shell”, which is located on the “settings” tab.

This public key will be required in the further course to configure the connection in DCC. Therefore, it is recommended to temporarily save/store this key, for example via a text file.



☑ SSH Secure Shell

Netzwerk Port: 22

□ Automatische Alarm- / Warnungsmeldungen immer senden

Netzwerkschnittstelle

☑ Ethernet 1

☑ Ethernet 2

Authentifizierung

○ Benutzername/Passwort ● Zertifikat

□ Debugging

SSH Zertifikat (Privat)

Zertifikat Passwort: ####

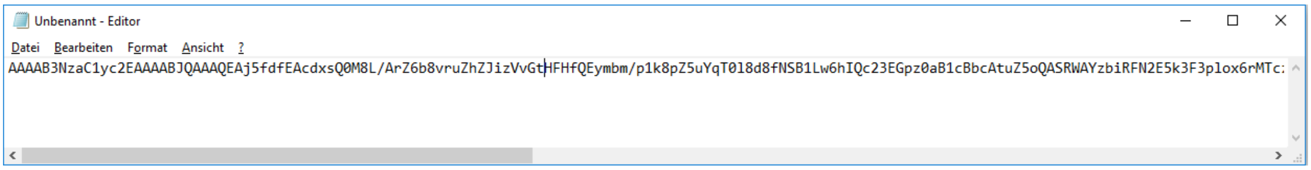
Willkommenstext

```
Hello SSH User, welcome to your NOX!
```

```
AAAAB3NzaC1yc2EAAAABJQAAAQEAj5fdfEAcdxsQ0M8L/ArZ6b8vruZhZJizVvGt
HFHfQEymbm/p1k8pZ5uYqT018d8fNSB1Lw6hIQc23EGpz0aB1cBbcAtuZ5oQASRW
AYzbiRFN2E5k3F3plox6rMTczLhiG86pIk7C6OiYF+VT2inOuVgEVqGyzE9pIKuN
6RljLVe3O4nWU7k54N0e3pCBzKm9UtaDaGX+6CPRwwiBDPWAEaLtLoEnz/IcLzZw
eKELDvHD6ybjhlymn3tzId/pSCqyi+pQPSEfvQDtf4cyiPUeqsljqV7ZR8TRxn3n
kITNbFtG5seKMgqkICPfpnd2Xxw3ivMqN8GVLH0diIr2ocglOw==
```

Figure 13: Temporary storage of the public key

Please remove the line breaks in the editor! This must be done, so that the public key will completely fit into one line.



```
AAAAB3NzaC1yc2EAAAABJQAAAQEAj5fdfEAcdxsQ0M8L/ArZ6b8vruZhZJizVvGtHFHfQEymbm/p1k8pZ5uYqT0l8d8fNSB1Lw6hIQc23EGpz0aB1cBbcAtuZ5oQASRWAYzbiRFN2E5k3F3plox6rMTc
```

Figure 14: Corrected public key format

!	***PLEASE NOTE***
	No connection to the SiInt is possible if the line breaks are not removed. **Please make sure not to remove any additional characters when removing the line breaks.**

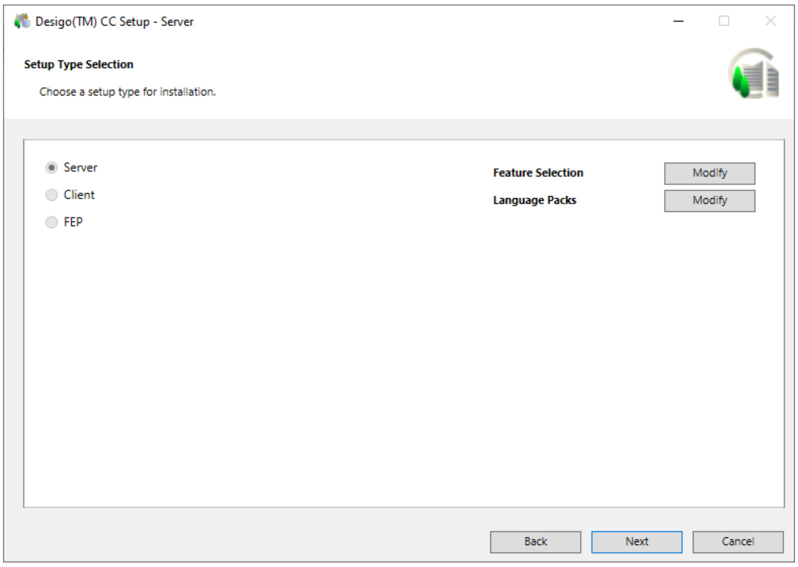
6 Installation of the Required Extension Modules (EM) DAIG_TrPro_049 and TranslinerLib_103

6.1.1 Dependencies to the Security Domain Libraries

The DCC-object models, which ae used for the SiInt-integration are dependent from the Security Domain Libraries. Therefore, these are a pre-requisite. If this EM is not yet part of the DCC-installation, it must be must installed first.

6.1.2 Installation of the Extension Modules

The extension modules DAIG_049, DAIG_TrPro_049 and TranslinerLib_103 will be installed via the Desigo CC Program Suite menu item named “Update Desigo CC”:



Desigo(TM) CC Setup - Server

Setup Type Selection

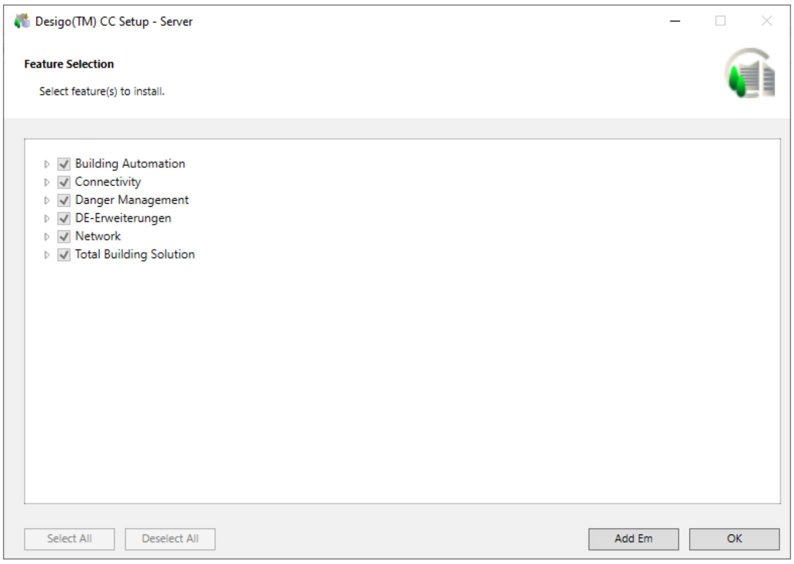
Choose a setup type for installation.

● Server
○ Client
○ FEP

Feature Selection Modify
Language Packs Modify

Figure 15: Update Desigo CC-Window

Execute: “Feature-Selection” -->”Modify“-Button



Desigo(TM) CC Setup - Server

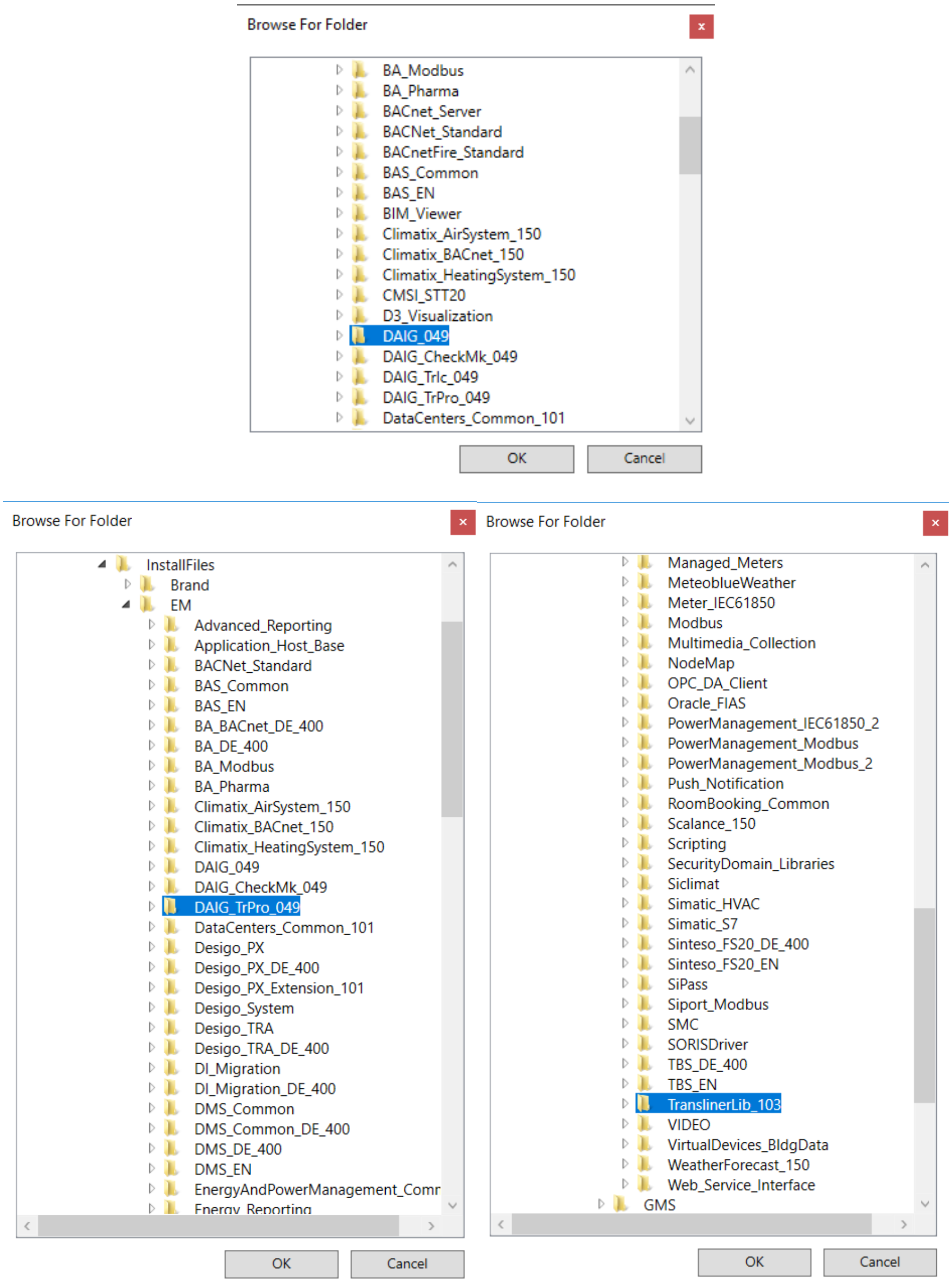
Feature Selection

Select feature(s) to install.

- ☑ Building Automation
- ☑ Connectivity
- ☑ Danger Management
- ☑ DE-Erweiterungen
- ☑ Network
- ☑ Total Building Solution

Figure 16: Update Desigo CC: Feature Selection

Confirm the “Add EM”-button. The „Add EM“ procedure must be repeated for each of the 3 EMs.



Browse For Folder

- BA_Modbus
- BA_Pharma
- BACnet_Server
- BACNet_Standard
- BACnetFire_Standard
- BAS_Common
- BAS_EN
- BIM_Viewer
- Climatix_AirSystem_150
- Climatix_BACnet_150
- Climatix_HeatingSystem_150
- CMSI_STT20
- D3_Visualization
- DAIG_049
- DAIG_CheckMk_049
- DAIG_Trlc_049
- DAIG_TrPro_049
- DataCenters_Common_101

Browse For Folder

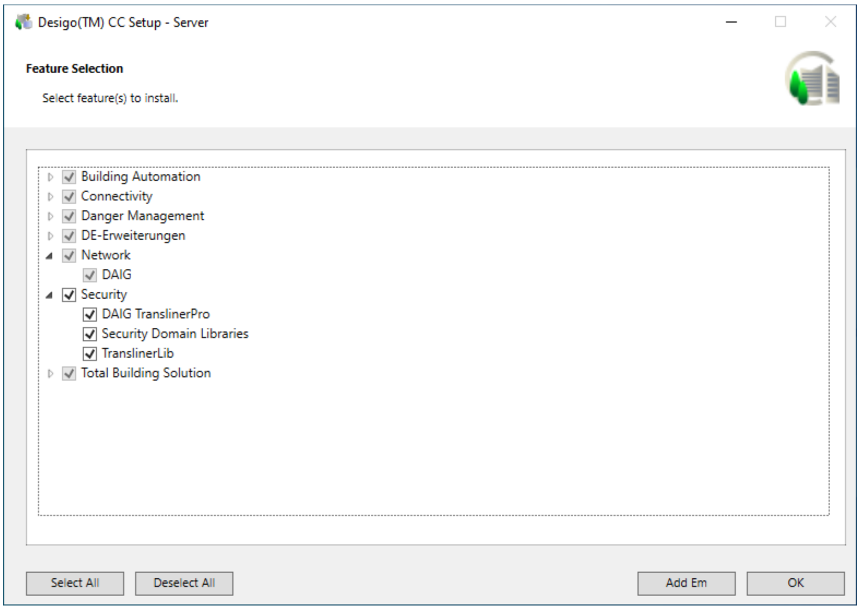
- InstallFiles
  - Brand
  - EM
    - Advanced_Reporting
    - Application_Host_Base
    - BACNet_Standard
    - BAS_Common
    - BAS_EN
    - BA_BACnet_DE_400
    - BA_DE_400
    - BA_Modbus
    - BA_Pharma
    - Climatix_AirSystem_150
    - Climatix_BACnet_150
    - Climatix_HeatingSystem_150
    - DAIG_049
    - DAIG_CheckMk_049
    - DAIG_TrPro_049
    - DataCenters_Common_101
    - Desigo_PX
    - Desigo_PX_DE_400
    - Desigo_PX_Extension_101
    - Desigo_System
    - Desigo_TRA
    - Desigo_TRA_DE_400
    - DI_Migration
    - DI_Migration_DE_400
    - DMS_Common
    - DMS_Common_DE_400
    - DMS_DE_400
    - DMS_EN
    - EnergyAndPowerManagement_Comr
    - Energy_Reporting

Browse For Folder

- Managed_Meters
- MeteoblueWeather
- Meter_IEC61850
- Modbus
- Multimedia_Collection
- NodeMap
- OPC_DA_Client
- Oracle_FIAS
- PowerManagement_IEC61850_2
- PowerManagement_Modbus
- PowerManagement_Modbus_2
- Push_Notification
- RoomBooking_Common
- Scalance_150
- Scripting
- SecurityDomain_Libraries
- Siclimat
- Simatic_HVAC
- Simatic_S7
- Sinteso_FS20_DE_400
- Sinteso_FS20_EN
- SiPass
- Siport_Modbus
- SMC
- SORISDriver
- TBS_DE_400
- TBS_EN
- TranslinerLib_103
- VIDEO
- VirtualDevices_BldgData
- WeatherForecast_150
- Web_Service_Interface
- GMS

Figure 17: Update Desigo CC: EM Selection

Please confirm each of the individual EMs via „OK“.



Desigo(TM) CC Setup - Server

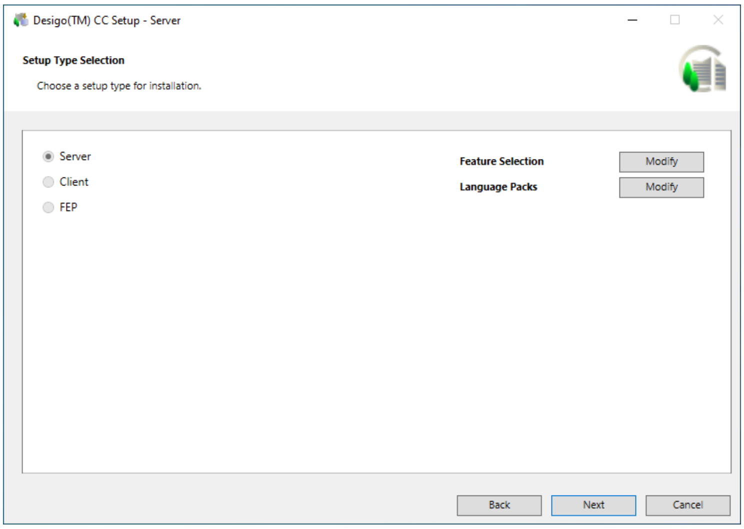
Feature Selection

Select feature(s) to install.

- ☑ Building Automation
- ☑ Connectivity
- ☑ Danger Management
- ☑ DE-Erweiterungen
- ☑ Network
  - ☑ DAIG
- ☑ Security
  - ☑ DAIG TranslinerPro
  - ☑ Security Domain Libraries
  - ☑ TranslinerLib
- ☑ Total Building Solution

Figure 18: Update Desigo CC: Selection of DAIG TranslinerPro, Security Domain Libraries, TranslinerLib

“Back” to Installer



Desigo(TM) CC Setup - Server

Setup Type Selection

Choose a setup type for installation.

- ● Server
- ○ Client
- ○ FEP

Feature Selection Modify

Language Packs Modify

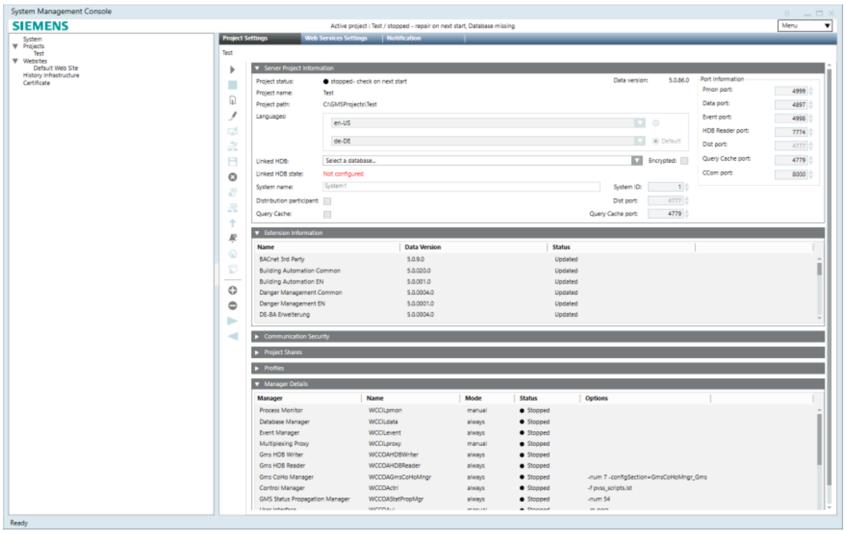
Figure 19: Update Desigo CC: Execute installation

Continue to navigate and execute the installation.

6.1.3 Add the Extension Module to the Project

!	***PLEASE NOTE***
	If adding an extension to an existing project, this project must be stopped first. **If creating a new project with the EM, this must be done during the configuration process.**

The extension modules DAIG TranslinerPro, TranslinerLib und Domain Security Libraries will be added to the project via the Desigo CC System Managment Console (SMC).



Active project : Test / stopped - repair on next start, Database missing

Project status: ● stopped- check on next start

Project name: Test

Project path: C:\GMSProjects\Test

Languages: en-US; de-DE ◉ Default

Linked HDB: Select a database...

Encrypted: □

Linked HDB state: Not configured

System name: System1

System ID: 1

Distribution participant: □

Dist port: 4777

Query Cache: □

Query Cache port: 4779

Data version: 5.0.86.0

Pmon port: 4999

Data port: 4897

Event port: 4998

HDB Reader port: 7774

Dist port: 4777

Query Cache port: 4779

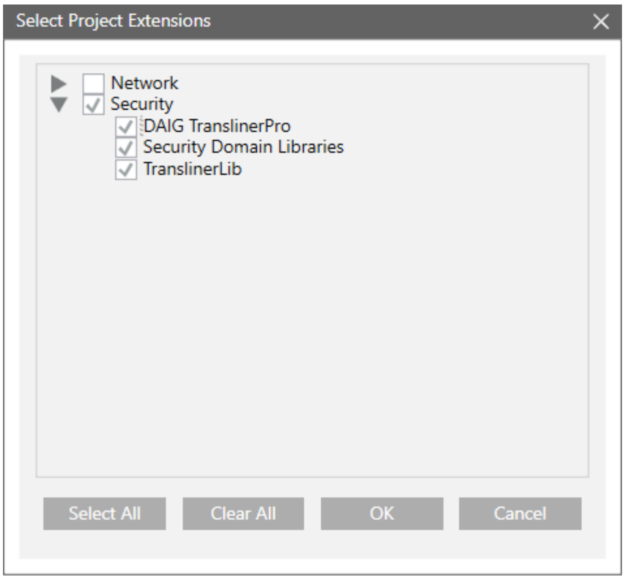
CCom port: 8000

Name	Data Version	Status
BACnet 3rd Party	5.0.9.0	Updated
Building Automation Common	5.0.020.0	Updated
Building Automation EN	5.0.001.0	Updated
Danger Management Common	5.0.0004.0	Updated
Danger Management EN	5.0.0001.0	Updated
DE-BA Erweiterung	5.0.0004.0	Updated

Manager	Name	Mode	Status	Options
Process Monitor	WCCILpmon	manual	● Stopped	
Database Manager	WCCILdata	always	● Stopped	
Event Manager	WCCILevent	always	● Stopped	
Multiplexing Proxy	WCCILproxy	manual	● Stopped	
Gms HDB Writer	WCCOAHDBWriter	always	● Stopped	
Gms HDB Reader	WCCOAHDBReader	always	● Stopped	
Gms CoHo Manager	WCCOAGmsCoHoMngr	always	● Stopped	-num 7 -configSection=GmsCoHoMngr_Gms
Control Manager	WCCOActrl	always	● Stopped	-f pvss_scripts.lst
GMS Status Propagation Manager	WCCOAStatPropMgr	always	● Stopped	-num 54

Figure 20: Adding the Extension Module

Please use/open the ⊕ -button dialogue to add EMs:



▶ □ Network
▼ ☑ Security
☑ DAIG TranslinerPro
☑ Security Domain Libraries
☑ TranslinerLib

Figure 21: Dialogue adding the extension module

Please select the DAIG SiInt-EM (Security Domain Libraries und TranslinerLib will be selected automatically) and confirm by clicking “OK”.

Click on the 💾 - Icon.

!	***PLEASE NOTE***
	If websites and web-applications are to be used within the project, an upgrade of these must occur after the installation or update of the DAIG-extension module!

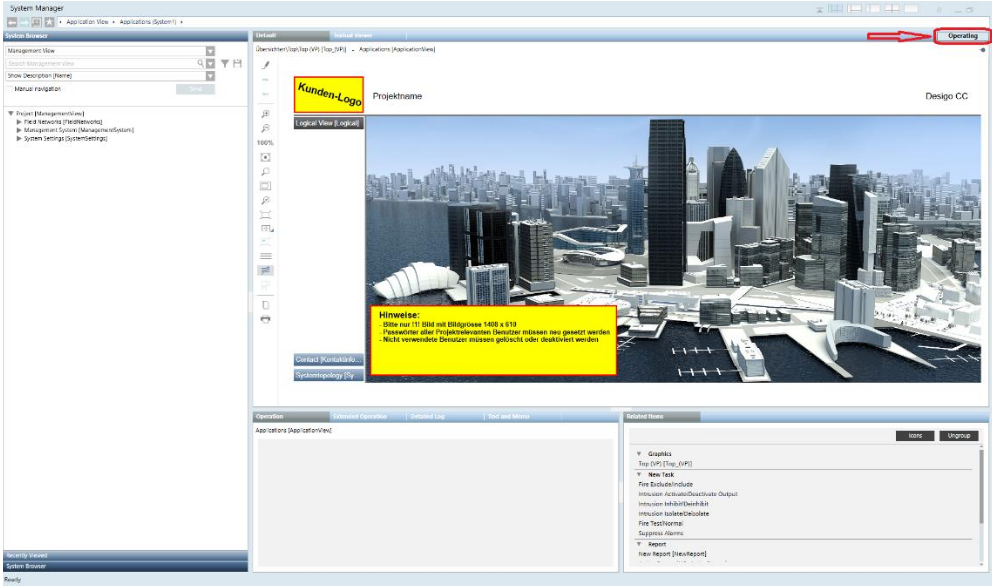
Please start the Desigo CC-project after adding the DAIG-extension module.

7 Configuration to Connect the SiInt-Interface to DCC

!	*PLEASE NOTE*
	The DCC user must have configurational rights to configure the SiInt-interface. All settings described below must be made in the configurational mode.

!	*PLEASE NOTE*
	For performance reasons, please set the transaction mode to „simple“ before doing bigger SiInt-transfers. **Upon completion of the import, this setting can be undone accordingly.**

Please switch to the configuration mode in DCC by clicking on “operation”.



Hinweise:
- Bitte nur !1! Bild mit Bildgrösse 1408 x 610
- Passwörter aller Projektrelevanten Benutzer müssen neu gesetzt werden
- Nicht verwendete Benutzer müssen gelöscht oder deaktiviert werden

Figure 22: Desigo CC-window switching in the configurational view

7.1.1 Adding a SiInt-Device

!	*PLEASE NOTE*
	The DAIG-driver must be started when performing all the below described configurational changes.

One SiInt-device-item can be added/created in the management-view underneath the tree-node for the DAIG-EM network, which was created during the installation.

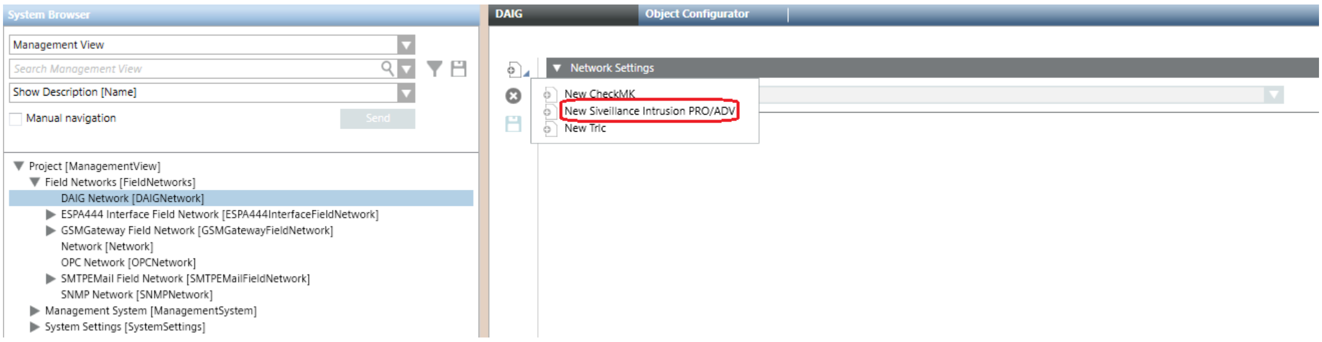
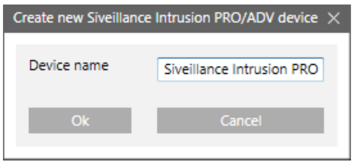

System Browser
Management View
Search Management View
Show Description [Name]
Manual navigation
Send
Project [ManagementView]
Field Networks [FieldNetworks]
DAIG Network [DAIGNetwork]
ESPA444 Interface Field Network [ESPA444InterfaceFieldNetwork]
GSMGateway Field Network [GSMGatewayFieldNetwork]
Network [Network]
OPC Network [OPCNetwork]
SMTPEMail Field Network [SMTPEMailFieldNetwork]
SNMP Network [SNMPNetwork]
Management System [ManagementSystem]
System Settings [SystemSettings]
DAIG
Object Configurator
Network Settings
New CheckMK
New Siveillance Intrusion PRO/ADV
New Tric

Figure 23: Desigo CC: Creating/Adding a New SiInt-Device

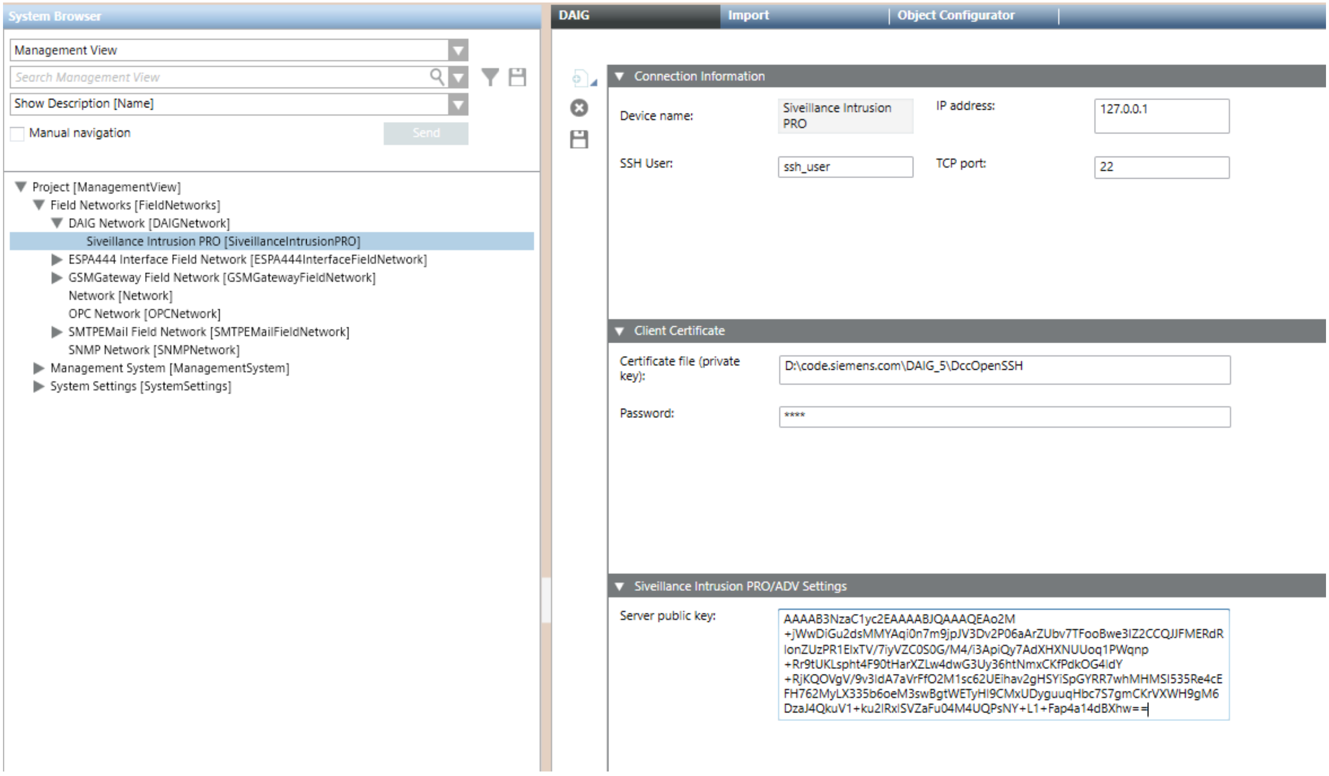


Device name: Siveillance Intrusion PRO

Figure 24: Desigo CC: Dialogue, Creating/Adding a New SiInt-Device

7.1.2 Configuration of the Connection to SiInt & Configuring the Polling-Parameter as well as the Log-Level

The connection to SiInt will be configured in the newly created/added device-tree-node in the “DAIG”-register.


System Browser
Management View
Search Management View
Show Description [Name]
Manual navigation
Send
Project [ManagementView]
Field Networks [FieldNetworks]
DAIG Network [DAIGNetwork]
Siveillance Intrusion PRO [SiveillanceIntrusionPRO]
ESPA444 Interface Field Network [ESPA444InterfaceFieldNetwork]
GSMGateway Field Network [GSMGatewayFieldNetwork]
Network [Network]
OPC Network [OPCNetwork]
SMTPEMail Field Network [SMTPEMailFieldNetwork]
SNMP Network [SNMPNetwork]
Management System [ManagementSystem]
System Settings [SystemSettings]
DAIG
Import
Object Configurator
Connection Information
Client Certificate
Siveillance Intrusion PRO/ADV Settings

Device name: Siveillance Intrusion PRO

IP address: 127.0.0.1

SSH User: ssh_user

TCP port: 22

Certificate file (private key): D:\code.siemens.com\DAIG_5\DccOpenSSH

Password: ****

Server public key:

```
AAAAB3NzaC1yc2EAAAABJQAAAQEAo2M
+jWwDiGu2dsMMYAqi0n7m9jpJV3Dv2P06aArZUbv7TFooBwe3IZ2CCQJJFMERdR
lonZUzPR1ElxTV/7iyVZC0S0G/M4/i3ApiQy7AdXHXNUUoq1PWqnp
+Rr9tUKLspht4F90tHarXZLw4dwG3Uy36htNmxCKfPdkOG4ldY
+RjKQOVgV/9v3ldA7aVrFfO2M1sc62UEihav2gHSYiSpGYRR7whMHMSI535Re4cE
FH762MyLX335b6oeM3swBgtWETyHI9CMxUDyguuqHbc7S7gmCKrVXWH9gM6
DzaJ4QkuV1+ku2lRxlSVZaFu04M4UQPsNY+L1+Fap4a14dBXhw==
```

Figure 25: Desigo CC: Connection-Configuration to SiInt

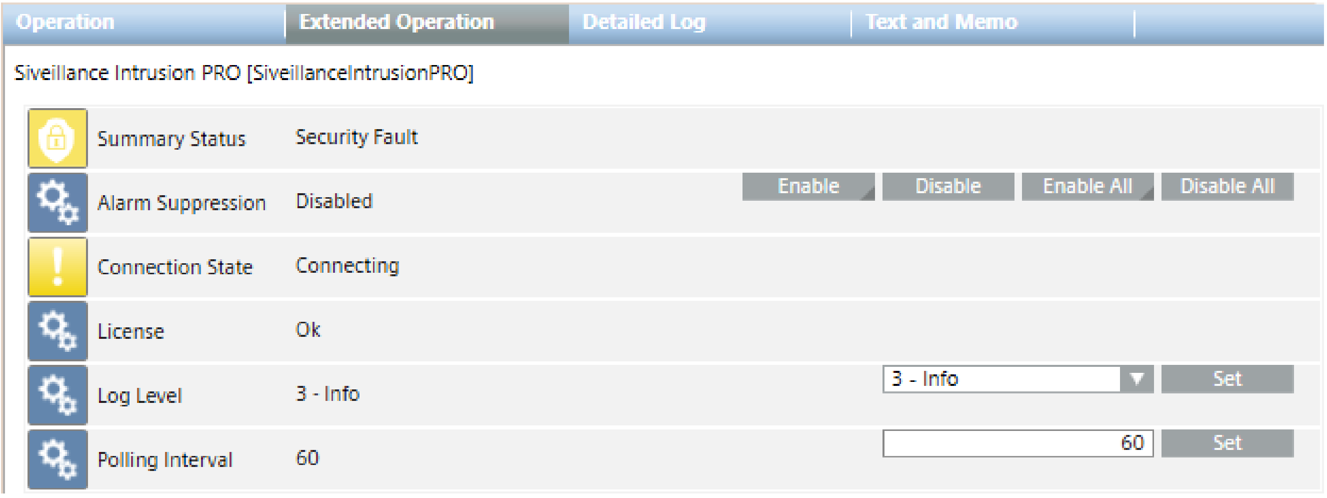
The configuration of the SiInt-device includes the following parameters:

- IP-address of the local monitoring-entity (no hostname!)

- User for the encrypted connection to SiInt (will be configured within SiInt)
- TCP-Port of the connection (SSH: 22)
- Client-certificate-file on the DCC-computer, which was created in section0 (Clicking onto the field will open the “Windows”-explorer window to select the file)
- Password of the client-certificate-file
- Public SSH-key from SiInt in section 5.2.3 (**Pease ensure that the complete public key was truly and fully copied into the field!)**

After entering the parameter, please save the new configuration and wait until the connection to the SiInt-system is established (connection status: connected).

7.1.3 Adjusting the Poling-Time-Interval in the Extended Operation



Siveillance Intrusion PRO [SiveillanceIntrusionPRO]

Summary Status Security Fault

Alarm Suppression Disabled

Connection State Connecting

License Ok

Log Level 3 - Info — 3 - Info

Polling Interval 60 — 60

Figure 26: Desigo CC: Adjusting the Polling-Time-Interval

The polling-parameter determines the time-interval (in sec), as to when the SiInt-system will be queried for configurational changes. The standard value for the polling-parameter is 60 seconds. It can be changed under the menu-item “Extended Operation “.

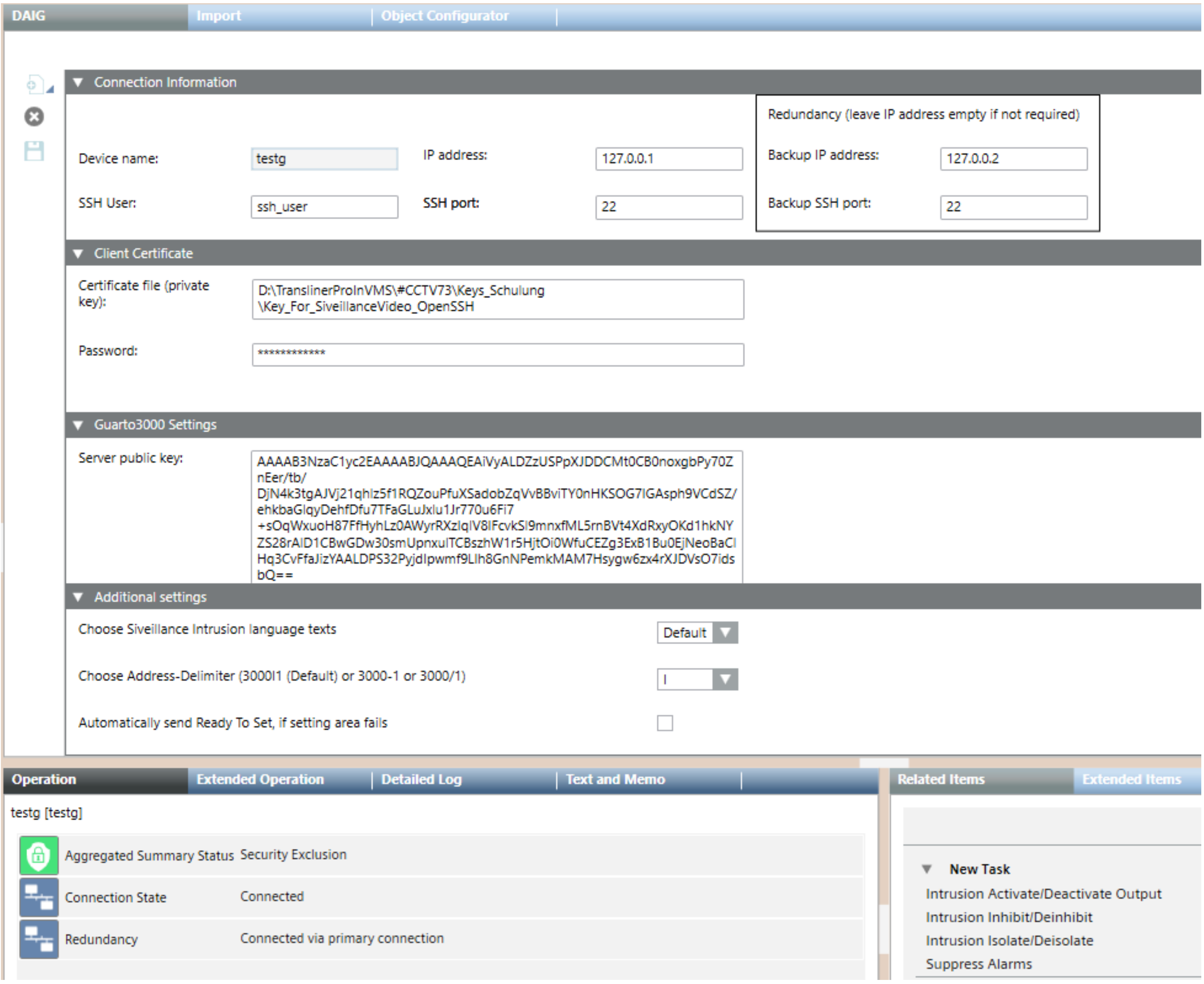
The duration of the log-level for the driver can be changed via “Extended Operations” as well generating more detailed log-data for review & analysis purposes. The log-levels can be combined with each other. Thus, for example the log-level 3 is activated as a standard, displaying a combination of EROR and WARNING.

Log-Level	**Integer-Value**	**Meaning**
ERR	1	Errors preventing the correct operation of the SiInt-connection
WARN	2	Warnings preventing a partially correct operation of the SiInt-connection
INFO	4	Overview/information to verify the correct operation
DBG	8	Detailed information for review & analysis purposes in case of faulty operation.

!	***PLEASE NOTE***
	If the SiInt-system is offline or if the network connection is disconnected, the DAIG-driver will periodically try to connect to the SiInt-system. Once connected successfully, all states and alarms will be synchronized with DCC.

7.1.4 Configuration of a redundant connection

If you want to use a redundant connection to the Siveillance Intrusion Pro system, you have to setup the Backup-IP-Address and Backup-Port. Due to same configuration on both redundant Siveillance Intrusion Pro-CPUs no further configuration information have to be changed.



Device name: testg

IP address: 127.0.0.1

SSH User: ssh_user

SSH port: 22

Redundancy (leave IP address empty if not required)

Backup IP address: 127.0.0.2

Backup SSH port: 22

Certificate file (private key): D:\TranslinerProInVMS\#CCTV73\Keys_Schulung\Key_For_SiveillanceVideo_OpenSSH

Password: ************

Server public key:

```
AAAAB3NzaC1yc2EAAAABJQAAAQEAiVyALDZzUSPpXJDDCMt0CB0noxgbPy70Z
nEer/tb/
DjN4k3tgAJVj21qhIz5f1RQZouPfuXSadobZqVvBBviTY0nHKSOG7lGAsph9VCdSZ/
ehkbaGlqyDehfDfu7TFaGLuJxlu1Jr770u6Fi7
+sOqWxuoH87FfHyhLz0AWyrRXzlqlV8IFcvkSl9mnxfML5rnBVt4XdRxyOKd1hkNY
ZS28rAlD1CBwGDw30smUpnxulTCBszhW1r5HjtOi0WfuCEZg3ExB1Bu0EjNeoBaCl
Hq3CvFfaJizYAALDPS32PyjdIpwmf9LIh8GnNPemkMAM7Hsygw6zx4rXJDVsO7ids
bQ==
```

Choose Siveillance Intrusion language texts: Default

Choose Address-Delimiter (3000I1 (Default) or 3000-1 or 3000/1): I

Automatically send Ready To Set, if setting area fails □

testg [testg]

🔒	Aggregated Summary Status	Security Exclusion
	Connection State	Connected
	Redundancy	Connected via primary connection

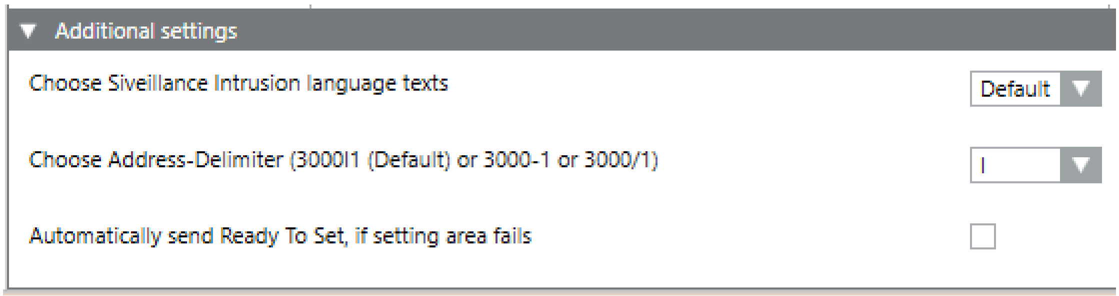
By using the redundancy function, the “Redundancy”-Datapoint will be activated. This datapoint can be found on the Siveillance Intrusion Pro device node and will display the state of the redundant connection. Following states are possible:

- Normal
- Connected via backup connection (Primary connection lost)
- Connected via backup connection (Primary connection available)
- Connected (Backup connection lost)
- Disconnected (Primary and backup connection lost)
- No redundancy in use

!	*PLEASE NOTE*
	In order to use the redundancy function, two licenses for the Siveillance Intrusion Pro integration in Desigo CC is required.

7.1.5 Configuration of detector- and area language texts for the import

The intrusion panel supports several languages. If you want to use different language texts than the default language (configured in the intrusion panel), you can select to preferred language for detector and area names in the configuration view of the interface.



▼ Additional settings

Choose Siveillance Intrusion language texts: Default

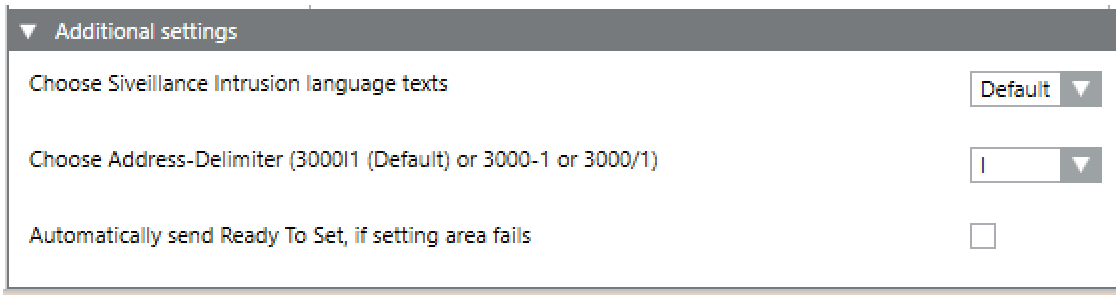
Choose Address-Delimiter (3000|1 (Default) or 3000-1 or 3000/1): |

Automatically send Ready To Set, if setting area fails ☐

If the given language is not available in the intrusion panel, the interface will automatically fall back to the standard language texts from the intrusion panel.

7.1.6 Configuration of the address delimiter for detectors

Detector addresses of the intrusion panel are set as ID of the detector nodes in Desigo CC. For configuration of the delimiter character between the unit address and the input number from the intrusion panel, simply select the preferred character in the configuration view of the interface. Available characters area | , - or / .



▼ Additional settings

Choose Siveillance Intrusion language texts: Default

Choose Address-Delimiter (3000|1 (Default) or 3000-1 or 3000/1): |

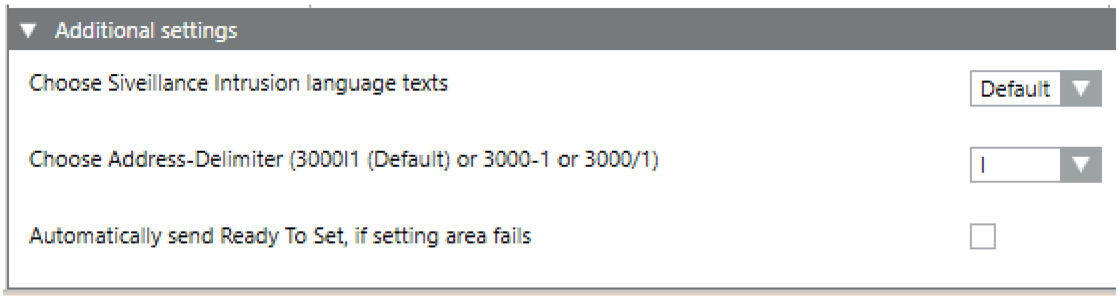
Automatically send Ready To Set, if setting area fails ☐

!	*PLEASE NOTE*
	Changing the address delimiter will result in having to reimport every detector and losing references on graphics.

7.1.7 Automated Ready to Set

After trying and failing to set an area from Desigo CC, you can configure to automatically send an Ready to Set command. By checking the „automatically send Ready to Set, if setting area fails” checkbox this function is activated.

The feedback of this automated Ready to Set command is the same as if the user presses the Ready to Set button.



▼ Additional settings

Choose Siveillance Intrusion language texts: Default

Choose Address-Delimiter (3000I1 (Default) or 3000-1 or 3000/1): I

Automatically send Ready To Set, if setting area fails: □

7.1.8 Import of the SiInt-Configuration

The SiInt-interface supports the online configuration method. This means, that once successfully connected, the SiInt-connection will be transferred automatically. No configurational files must be imported into DCC.

The import of an intrusion model from the SiInt-configuration consists the following steps:

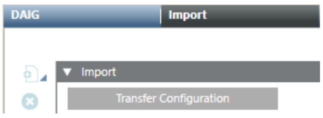
1. Transfer the SiInt-configuration into DCC
2. Use the configurational tree-nodes to select the areas, detectors, hardware-modules, etc., which are to be imported
3. Import the selected objects into DCC: Create/add the datapoint and nodes in the management-tree

The SiInt-interface periodically polls the system for configurational changes. Please perform the above-mentioned steps 1-3 once again as soon as a change in the configuration is detected.

Steps 2-3 can be performed at any time if either areas / detectors etc. are to be deleted or added to the interface-connection.

The following sections will provide further details to the individual steps.

7.1.8.1 Copy the Configuration from the Siveillance Intrusion PRO/ADV System



During the first-time configuration and during every configurational change, the SiInt module of the DAIG-driver imports the SIint-configuration. This activates the button **“Transfer configuration from SiInt”** within the “import”-tab of the SiInt-device configuration. Clicking on this button will import the new SiInt-configuration adding it to the configurational tree-node-view and deleting objects, which are no longer available.

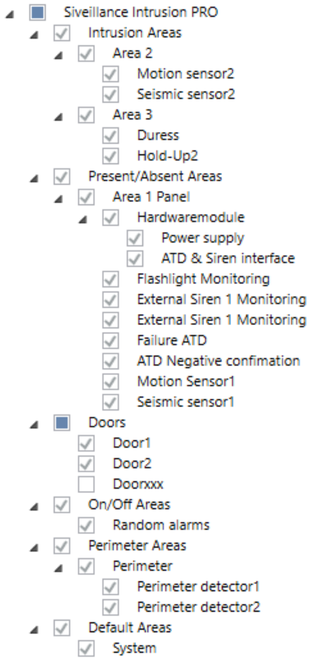
The result of this procedure is a new configurational tree-view activating the button **“transfer configuration from SiInt”** again.

!	***PLEASE NOTE***
	The SiInt-module in the DAIG driver periodically polls the SiInt-system for configurational changes. The standard value for the time-interval is 60 seconds. It can be changed via the device-settings of the SiInt-device (please see above).

The polling-parameter determines the time-interval (in sec), as to when the SiInt-system will be queried for configurational changes. The standard value for the polling-parameter is 60 seconds. It can be changed under the menu-item “Extended Operation“.

!	**If a new SiInt-configuration is not transferred, the SiInt-connection including the very last existing configurations will be run.** **Command & control functions, status-displays and the alarming of existent areas / detectors etc. will still function. However new areas/detectors etc. will no longer be available.** **Also, the tree-nodes of deleted areas/detectors will be displayed. Thus, the connection will become inconsistent. Therefore, it is advisable, to immediately transfer new configurations into DCC, once changes in the SiInt-configuration take place.**

7.1.8.2 Select those Objects in the Configuration-Tree, which are to be Imported



- ■ Siveillance Intrusion PRO
  - ☑ Intrusion Areas
    - ☑ Area 2
      - ☑ Motion sensor2
      - ☑ Seismic sensor2
    - ☑ Area 3
      - ☑ Duress
      - ☑ Hold-Up2
  - ☑ Present/Absent Areas
    - ☑ Area 1 Panel
      - ☑ Hardwaremodule
        - ☑ Power supply
        - ☑ ATD & Siren interface
      - ☑ Flashlight Monitoring
      - ☑ External Siren 1 Monitoring
      - ☑ External Siren 1 Monitoring
      - ☑ Failure ATD
      - ☑ ATD Negative confimation
      - ☑ Motion Sensor1
      - ☑ Seismic sensor1
  - ■ Doors
    - ☑ Door1
    - ☑ Door2
    - ☐ Doorxxx
  - ☑ On/Off Areas
    - ☑ Random alarms
  - ☑ Perimeter Areas
    - ☑ Perimeter
      - ☑ Perimeter detector1
      - ☑ Perimeter detector2
  - ☑ Default Areas
    - ☑ System

Figure 27: Desigo CC: SiInt- Configuration-Tree

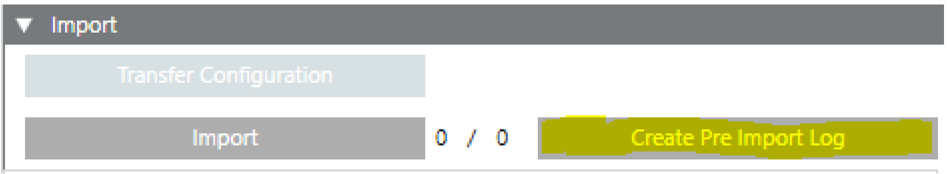
The intrusion areas (security areas, doors, HW-modules, detectors, etc.), which are available for the import will be displayed in a hierarchic structure by the configuration-tree in accordance with the way, these were aligned during the import within the DCC management-tree-view. The intrusion objects, that are to be imported can be selected via the checkboxes. Selecting or de-selecting an area will either select or deselect the detectors included. Selecting or deselecting the SiInt-tree-node will select or deselect all subordinate areas including detectors and HW-modules.

Objects, which are marked orange do indicate a change that took place since the last SIInt-configuration (such as name changes, structural changes of an additional entry).

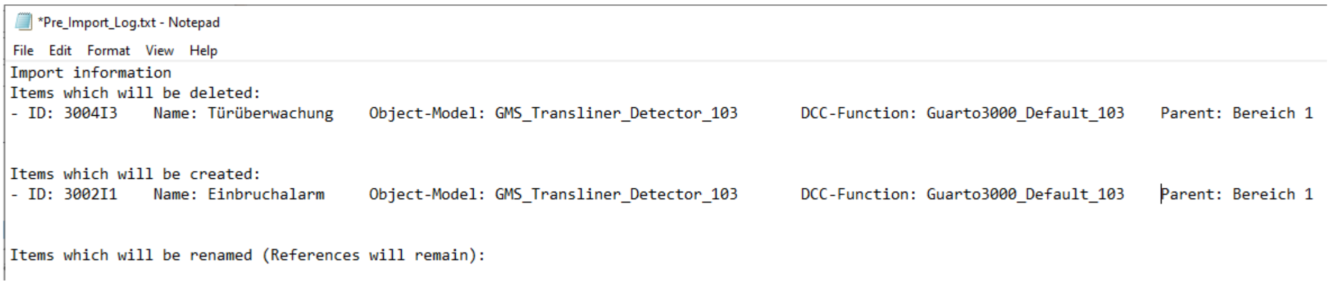
7.1.8.3 Generating a Pre-Import log

To view changes that would be applied once you import, you can generate an Pre Import Log. In this file all objects which would be deleted, created or renamed by an import will be listed.

The Pre-Import Log can be generated by pressing the „Generate Pre Import Log“.



The resulting file is available in the following directory „GMSMainProject/bin/DAIG_PreImportInformation“. You can also open it in the information message after generating the file.



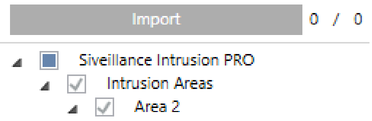
```
Import information
Items which will be deleted:
- ID: 3004I3    Name: Türüberwachung    Object-Model: GMS_Transliner_Detector_103       DCC-Function: Guarto3000_Default_103    Parent: Bereich 1


Items which will be created:
- ID: 3002I1    Name: Einbruchalarm     Object-Model: GMS_Transliner_Detector_103       DCC-Function: Guarto3000_Default_103    Parent: Bereich 1


Items which will be renamed (References will remain):
```

7.1.8.4 Import of selected objects in DCC

As soon as changes to the existing configuration are detected by the configuration -tree, the **Import**-Button will be activated importing the selected configuration into DCC.



After clicking on the Import-button, a reconnection to SiInt will take place synchronizing the imported states and alarms with those of the SiInt-system.

!	***PLEASE NOTE***
	A maximum system configuration of 5000 intrusion nodes distributed to a maximum of 5 Siveillance Intrusion PRO/ADV control panels were tested. **Larger systems are possible and subject to project-specific requests for validation. Also, please note the following points for larger systems:** • Creating/deleting a tree-node during the import takes between 0.05-1 sec. The progress is displayed next to the “Import”-button. Please remain in the “Import”-screen, until the import is fully completed! • Such a large configuration, as this one, only has a minor impact on the operational mode of the integration/connection: Starting the driver and establishing the connection including resync of alarms will only take few seconds.

!	***PLEASE NOTE***
	The "Import" button will be activated, if the configuration tree will change for any of the following reasons: • **A new SiInt PRO/ADV configuration is transferred** • **The DCC-user will select/deselect objects in the configuration-tree** **By confirming the now activated "Import" button, these configurational changes will be applied, and the selected/deselected DCC-tree-nodes will either appear/disappear accordingly.**

!	***PLEASE NOTE***
	All alarms of the SiInt PRO/ADV system are based on inputs. In DCC the inputs are displayed/mapped to as hardware modules or detectors. **If a hardware module/detector is excluded from the import, the alarms of its inputs will NOT be forwarded to DCC!**

!	***PLEASE NOTE***
	Objects, which are marked orange do indicate a change to the object, that took place since the last SIInt-configuration (such as name changes, structural changes of an additional entry). **During the import, this object will be deleted and newly added, erasing the history for this object.**

7.1.9 Individual Customizing

7.1.9.1 Adjustment of area type mappings

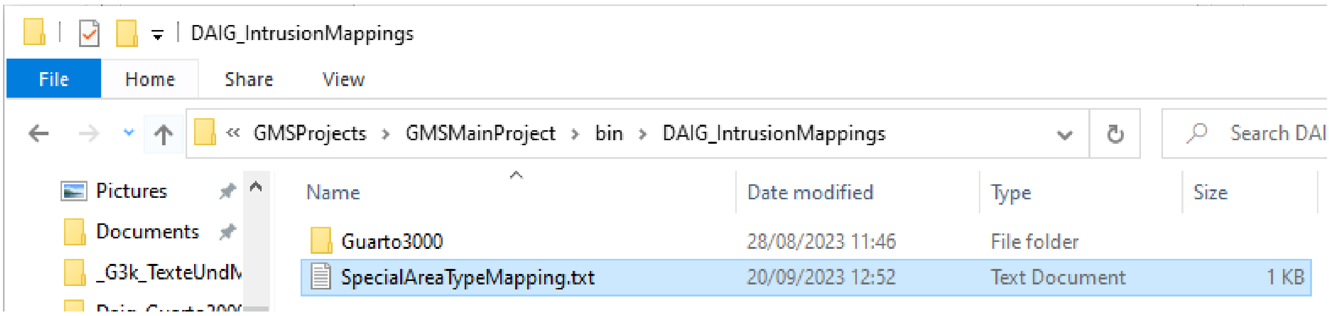
If the Siveillance Intrusion Pro panel is created without an template or the area type IDs were changed, you can adjust the mapping of area type IDs to Desigo CC area models.

The drivers uses the following default mapping:

Area type-ID	Desigo CC area type
0	Generic area type
1	Standard area
2	Door
3	On Off area
4	Present-/Absent area
5	Lock gate area
6	Gate area
7	Free Occupied area
8	Passage door

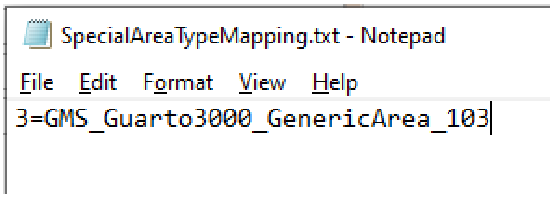
Every area type ID > 8 will be automatically mapped to the generic area type.

For adjusting the mapping, create the file „SpecialAreaTypeMapping.txt“ in the following directory: „GMSProjects\GMSMainProject\bin\DAIG_IntrusionMappings“.



Name	Date modified	Type	Size
Guarto3000	28/08/2023 11:46	File folder	
SpecialAreaTypeMapping.txt	20/09/2023 12:52	Text Document	1 KB

To change the mapping of the area type ID 3 (from the intrusion panel configuration) to the generic area type in Desigo CC use the following syntax:



```
3=GMS_Guarto3000_GenericArea_103
```

Following area type names in Desigo CC are valid values for the name of the model in the file:

- GMS_Guarto3000_GenericArea_103	-> Generic area type
- GMS_Guarto3000_StandardArea_103	-> Standard area
- GMS_Guarto3000_DoorArea_103	-> Door
- GMS_Guarto3000_OnOffArea_103	-> On Off area
- GMS_Guarto3000_PresentAbsentArea_103	-> Present Absent area
- GMS_Guarto3000_LockArea_103	-> Lock area
- GMS_Guarto3000_LockGateArea_103	-> Lock Gate area
- GMS_Guarto3000_FreeOccupiedArea_103	-> Free Occupied area
- GMS_Guarto3000_PassageDoor_103	-> Passage door

If the IDs for area states and commands are also configured on the project site please use the generic area type. This type uses a fully generic approach and has no dependencies to static area states

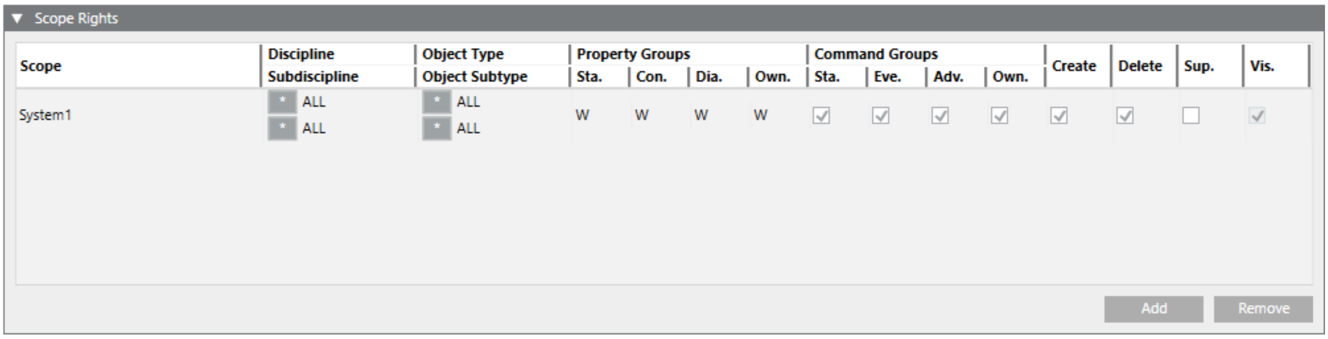
!	***PLEASE NOTE***
	After adjusting the area type mapping, the driver has the be restarted to reflect the changes in Desigo CC.

7.1.9.2 Command & Control Authorizations

The command & control authorizations for intrusion areas, detectors etc. are set via DCC in the following manner:

- All users are allowed to conduct „Ready-to-Set“-Test, walk-tests, seismic-tests and sabotage-tests.
- The remaining command & control functions is limited to users, who have the command-group authorization „Extended“, such as:

- Set/unset intrusion areas
- Switch on/off detectors or HW-modules
- Open/close doors
- Switch on/off “On-/Off-Areas”



▼ Scope Rights

Scope	Discipline Subdiscipline	Object Type Object Subtype	Property Groups				Command Groups				Create	Delete	Sup.	Vis.
			Sta.	Con.	Dia.	Own.	Sta.	Eve.	Adv.	Own.				
System1	* ALL * ALL	* ALL * ALL	W	W	W	W	☑	☑	☑	☑	☑	☑	☐	☑

Command-Group Authorizations for DCC-user

7.1.9.3 Customization of Alarm-Mappings

If there are new Alarmtypes defined in the Siveillance Intrusion Pro configuration you have to additionally map these Alarmtypes for the Desigo CC interface. After starting the DAIG-Driver you can find the AreaAlarmMapping.txt and DetectorAlarmMapping.txt in the following directory: „GMSMainProject\bin\DAIG_IntrusionMappings\Guarto3000“

If you want to use a specific Alarmtype-ID for a detector your have to add the new Alarmtype-ID and map it to a Textgroup-ID, which is available in the detector alarm table (in DCC).

After restarting the driver, the new Alarmtype-Mapping will be used.

!	***PLEASE NOTE***
	After changing the alarm mapping, the driver must be restarted!

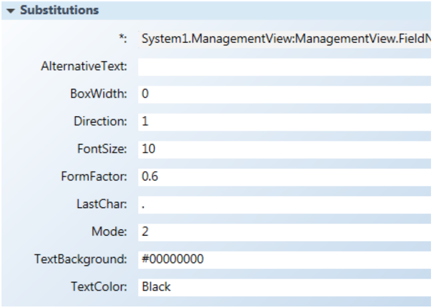
7.1.9.4 Individual Customizing of Alarms

As explained in section 4.2.3, the alarm-behavior is determined by the alarm-tables of the management-station-alarms or the field-system alarms used in the corresponding objects. These can be adjusted by standard DCC-procedures (customization) in accordance with project-specific-requirements.

!	***PLEASE NOTE***
	If alarm-tables are customized in accordance with project-specific requirements, the driver must be re-started afterwards!

7.1.9.5 Individual Customizing of the Icon-Texts

Following a corresponding graphic-symbol from the “Global_Base_400_ZN_1 Library customization”, the following substitutions were adopted for the text individually customizing the contents and positions of the icon-texts:



Substitutions

*:	System1.ManagementView:ManagementView.FieldN
AlternativeText:	
BoxWidth:	0
Direction:	1
FontSize:	10
FormFactor:	0.6
LastChar:	.
Mode:	2
TextBackground:	#00000000
TextColor:	Black

- Alternative Text: If modes = 1 (see below), the text will be displayed underneath the icon
- BoxWidth: If different from 0, it will determine the width of the text-box
- Direction: 1: underneath the icon
  2: left from the icon
  3: over the icon
  4: right from the icon
- FontSize: Text size
- LastChar: Separation character, which extracts the name from the tree-node name. Example: „System1.ManagementView:ManagementView.FieldNetworks.DAIGNetwork.TranslinerPro.Detecor1“ will be extracted to ”vcenter“ by LastChar = “.“
- Mode: 0: Node-name according to the tree-display (description, name, description [name] or Name [description])
  1: Alternative Text
  2: Name (default) extracted from the tree-node-name via LastChar
- TextBackground: Background color of the text
- TextColor: Text color

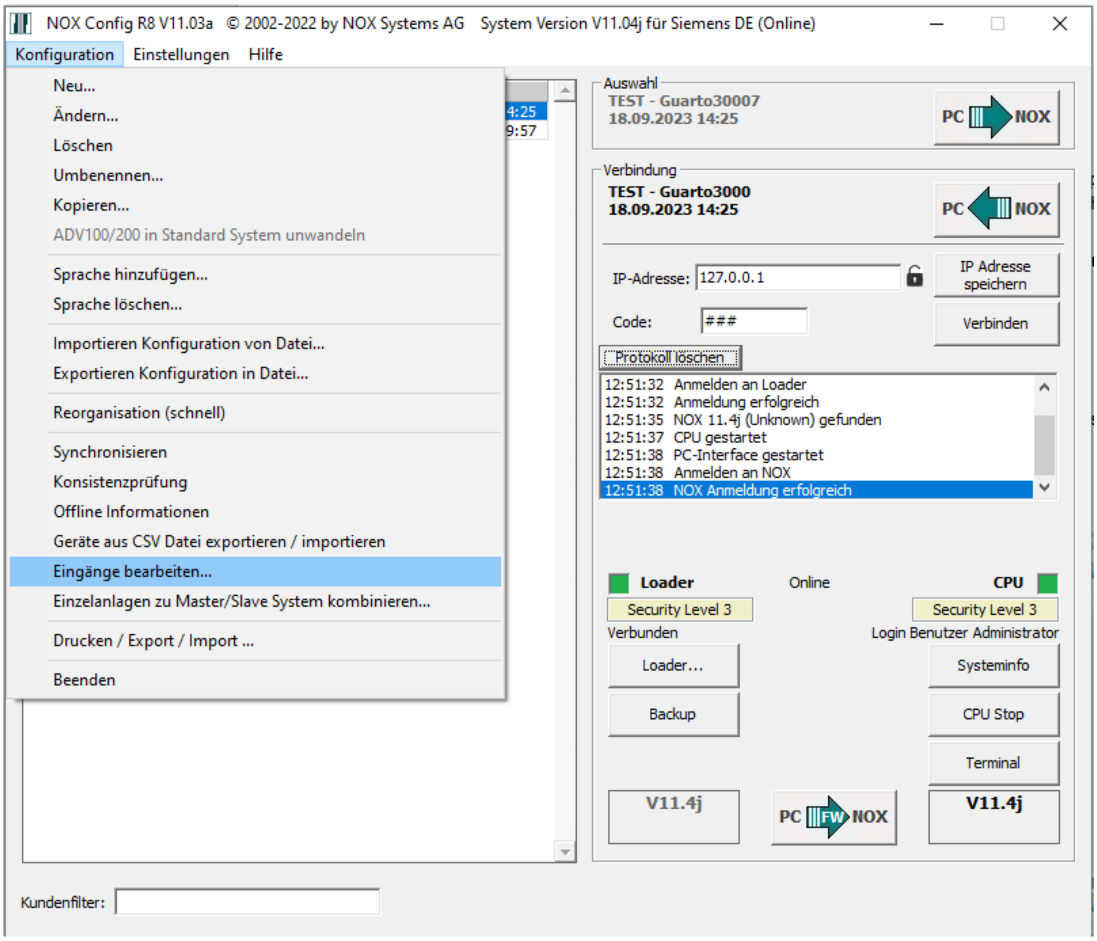
.

8 Troubleshooting

8.1 Faulty Siveillance Intrusion Pro Configuration

If there is an alarm in Desigo CC with the message „Guarto3000 configuration faulty“, check the Siveillance Intrusion Pro configuration for inconsistencies. In particular semicolons in input and area names lead to faulty configurations.

To check the input names you can use the function „change inputs“ in the configuration tool of the Siveillance Intrusion Pro.



NOX Config R8 V11.03a © 2002-2022 by NOX Systems AG System Version V11.04j für Siemens DE (Online)

Auswahl: TEST - Guarto30007 18.09.2023 14:25

Verbindung: TEST - Guarto3000 18.09.2023 14:25

IP-Adresse: 127.0.0.1

Code: ###

```
12:51:32  Anmelden an Loader
12:51:32  Anmeldung erfolgreich
12:51:35  NOX 11.4j (Unknown) gefunden
12:51:37  CPU gestartet
12:51:38  PC-Interface gestartet
12:51:38  Anmelden an NOX
12:51:38  NOX Anmeldung erfolgreich
```

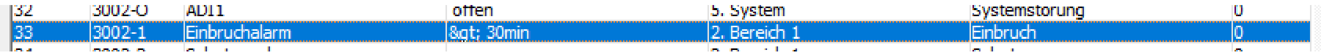
Loader: Verbunden

CPU: Login Benutzer Administrator

V11.4j

V11.4j

Example for a faulty input name:

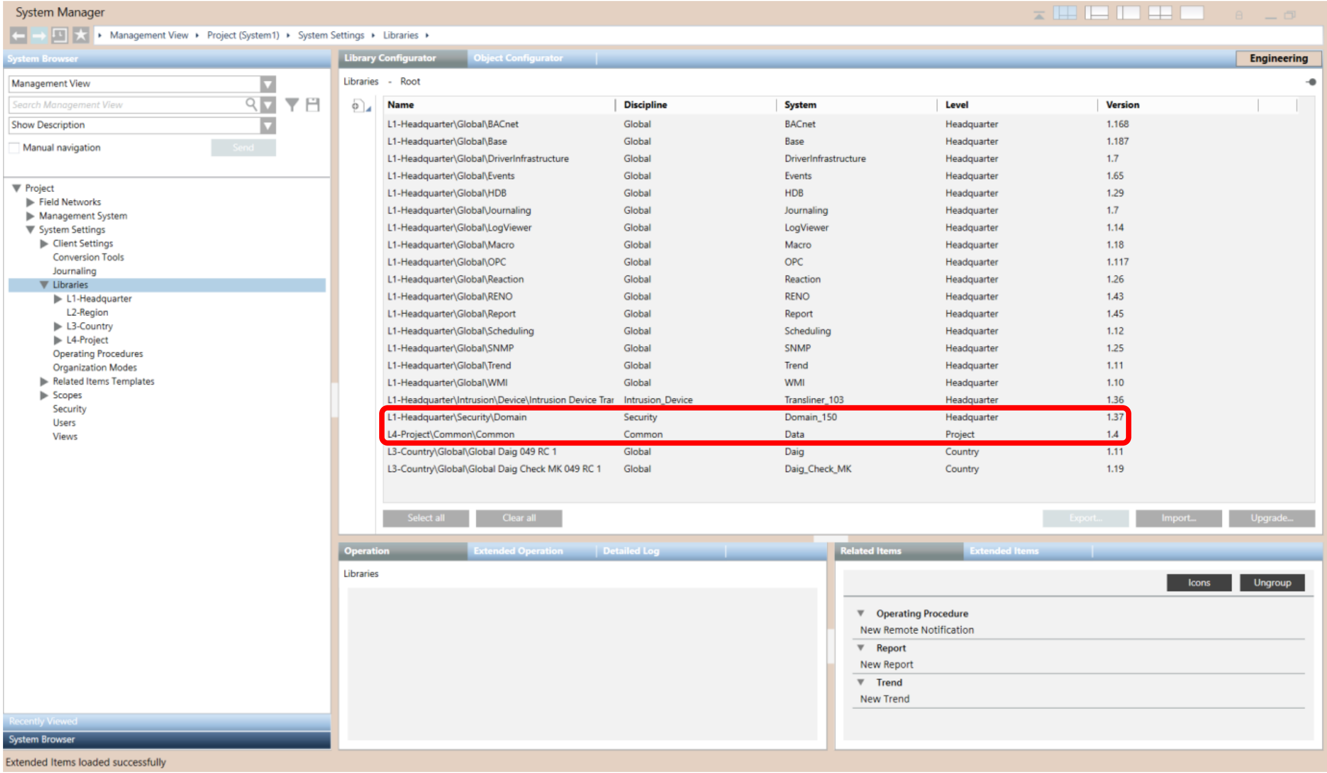


32	3002-0	AD11	offen	5. System	Systemstorung	0
33	3002-1	Einbruchalarm	&gt; 30min	2. Bereich 1	Einbruch	0

8.2 Verifying the correct Integration of EMs

Upon correct installation of the DAIG-TranslinerPro-EM, the following libraries are visible in the browser, under management view, in system settings/libraries:

- Intrusion_Device Transliner_103
- Security Domain_150



Name	Discipline	System	Level	Version
L1-Headquarter\Global\BACnet	Global	BACnet	Headquarter	1.168
L1-Headquarter\Global\Base	Global	Base	Headquarter	1.187
L1-Headquarter\Global\DriverInfrastructure	Global	DriverInfrastructure	Headquarter	1.7
L1-Headquarter\Global\Events	Global	Events	Headquarter	1.65
L1-Headquarter\Global\HDB	Global	HDB	Headquarter	1.29
L1-Headquarter\Global\Journaling	Global	Journaling	Headquarter	1.7
L1-Headquarter\Global\LogViewer	Global	LogViewer	Headquarter	1.14
L1-Headquarter\Global\Macro	Global	Macro	Headquarter	1.18
L1-Headquarter\Global\OPC	Global	OPC	Headquarter	1.117
L1-Headquarter\Global\Reaction	Global	Reaction	Headquarter	1.26
L1-Headquarter\Global\RENO	Global	RENO	Headquarter	1.43
L1-Headquarter\Global\Report	Global	Report	Headquarter	1.45
L1-Headquarter\Global\Scheduling	Global	Scheduling	Headquarter	1.12
L1-Headquarter\Global\SNMP	Global	SNMP	Headquarter	1.25
L1-Headquarter\Global\Trend	Global	Trend	Headquarter	1.11
L1-Headquarter\Global\WMI	Global	WMI	Headquarter	1.10
L1-Headquarter\Intrusion\Device\Intrusion Device Trar	Intrusion_Device	Transliner_103	Headquarter	1.36
L1-Headquarter\Security\Domain	Security	Domain_150	Headquarter	1.37
L4-Project\Common\Common	Common	Data	Project	1.4
L3-Country\Global\Global Daig 049 RC 1	Global	Daig	Country	1.11
L3-Country\Global\Global Daig Check MK 049 RC 1	Global	Daig_Check_MK	Country	1.19

Operating Procedure
New Remote Notification
Report
New Report
Trend
New Trend

Figure 28: Desigo CC: Verifying the Correct EM-Installation

8.3 Connection Attempt between DAIG-Driver and SiInt

The log file (C:\GMSProjects\<Projektname>\log: WCCOADAIGDriverX.log) shows if an attempt to connect to the SiInt-system was made:

```
WCCOADAIGDriver1:WCCOADAIGDriver(1), 2017.09.18 15:34:56.042,    INFO,   Opening connection to
trpro://127.0.0.1:22/1
```

A successful attempt will be displayed in the log:

```
WCCOADAIGDriver1:WCCOADAIGDriver(1), 2017.09.18 15:35:32.754,    INFO,   Connection to
trpro://127.0.0.1:22/1 succeeded
```

If the SiInt-system cannot be reached, the following log entry will be displayed:

```
WCCOADAIGDriver1:WCCOADAIGDriver(1), 2017.09.18 15:31:29.925,    WARN,   Connection to
trpro://127.0.0.1:22/1
```