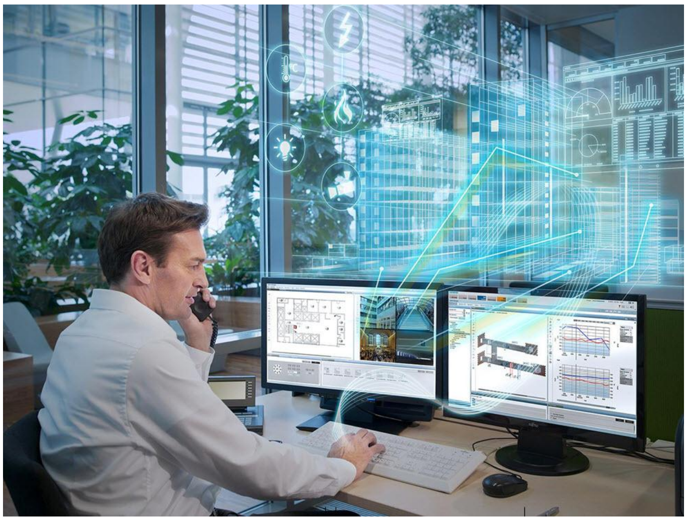
SIEMENS



# Desigo™ CC

# System Description Version 3.0 Extension Pack 1

Building Technologies

A6V10415500_en_b_30

2018-01-15

# Copyright Notice

## Notice

## Credits

Desigo, Desigo CC, Cerberus DMS, Cerberus PRO, and Sinteso are registered trademarks of Siemens Switzerland Ltd.

Other product or company names mentioned herein may be the trademarks of their respective owners.

Edition: 2018-02-06

Document ID: A6V10415500_en_b_30

# Table of Contents

# About This Document

## Purpose

This manual describes the Desigo CC management platform and gives the reader an overview of the system characteristics, the hardware and software requirements, the system limits and the approvals. It provides an overview to the supported system connectivity and the recommended system configurations.

## Scope

This document applies to Desigo CC Version 3.0 Extension Pack 1 (EP1).

## Target Audience

**Sales Representatives** are the first contact to the customer's buying center who establish the relationship. During pre-sales, they present the system to potential customers, focusing on unique selling propositions and benefits in order to acquire the project.

**Sales Engineers** provide pre- and post-sales technical advice and high-level support on product applications and solutions. They are often the key point of contact for clients, answering questions, providing technical advice and designing solutions. They have extensive knowledge of the products as well as the applications and network environments.

**Project Engineers** are responsible for planning and configuring a customer project. They provide the parameterization of products, devices, and systems and are responsible for general system troubleshooting. They have the appropriate training to their function and to the products, devices, and systems to be configured. They are familiar with the applied operating system(s) and the related network environment.

**Field Engineers** are responsible for commissioning at the customer site. They are trained appropriately to their function and to the products, devices, and systems to be installed. They are trained with the applied operating system(s) and the related network environment. Field engineers are responsible for infrastructure troubleshooting (for example, hardware, communication, network, and so on).

## How to use it

This document is organized as follows:

**Part A:** provides an overview of the applications, features, system architecture and Cyber security concepts. Please read it to obtain a basic knowledge of the product and to become familiar with key security aspects.

**Part B:** provides the guidelines and illustrates the tools for sizing the hardware platforms on which Desigo CC can run properly, depending on project requirements. It shall help to design the system.

**Part C:** describes detailed and binding specifications for several aspects of system configuration, like system limits, reference hardware configurations, IT environment compatibility, hardening guidelines and more. It can be used to verify project specification.

**Part D:** provides information for typical multi-discipline configurations that could be taken as a reference. These are typical uses cases with a certain amount of data points for the different disciplines. Note that the figures in this section do not indicate the system limits.

## Liability Disclaimer

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly and any necessary corrections included in subsequent editions. Suggestions for improvement are welcome.

## IT-Security Disclaimer

Siemens products and solutions provide IT-specific security functions to ensure the secure operation of building comfort, fire safety, security management and physical security systems. The security functions on these products and solutions are important components of a comprehensive security concept.

However, it is necessary to implement and maintain a comprehensive, state-of-the-art security concept that is customized to individual security needs. Such a security concept may result in additional site-specific preventive action to ensure that the building comfort, fire safety, security management or physical security systems for your site are operated in a secure manner. These measures may include, but are not limited to, separating networks, physically protecting system components, user awareness programs, in-depth security, and so on.

In this document, refer to the *Cyber Security Concepts* and to the

*Hardening Guidelines for Desigo CC* Deployments sections.

For additional information on IT security, please contact your Siemens sales or project department.

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/innovation/en/technology-focus/siemens-cert/cert-security-advisories.htm

# Document Revision History

## Document Identification

The document ID is structured as follows:

ID_Language(COUNTRY)_ModificationIndex_ProductVersionIndex

Example: A6Vnnnnnnnn_en_a_02

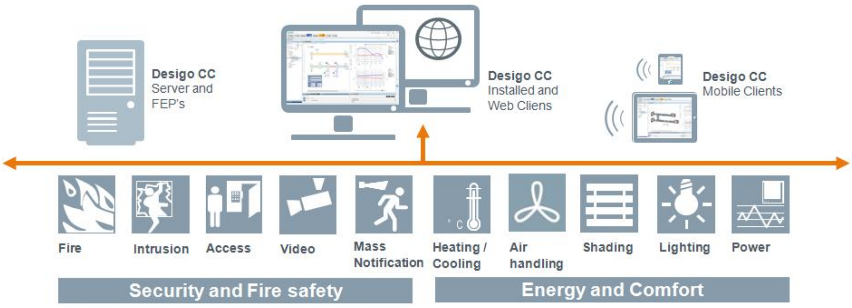
| Document Revision History. | | |
|---|---|---|
| **Modification Index** | **Edition Date** | **Brief Description** |
| a | 2017-07-15 | Final edition for the version 3.0 |
| b | 2018-01-15 | Updates ad corrections. Features coming with Extension Pack 1 have been included |

# 1 Part A: System Description

The Desigo CC management platform presents a single point of entry for users to operate, monitor and optimize building automation, fire safety and security systems or a combination thereof.

Desigo CC is a flexible, full client-server architecture allowing scalability from small and medium to large and complex systems. The platform provides customizable- and market-specific distributions.

Desigo CC can be installed on one single computer, with full server and client functionality. Furthermore, Installed, Web, and Windows App Clients can also be added on separate hardware. Additional system connections can be made through systems installed with Desigo CC Front End Processors (FEP) configurations. Web interfaces provide the customer an increased flexibility for operation and future extensions, e.g. mobile applications for tablets and smart phones.



## What's new?

- SORIS, Southbound Open RESTful Integration Service: subsystem integration
- Supporting tools and workflows for Desigo Insight, MM8000, Siclimat-X replacement and migration
- Extended support for Apogee Insight replacement and migration
- Graphics generator for Desigo PX (CAS library)
- Desigo system backwards compatibility (FW≥2.37)
- Meter Management
- Support for the integration, supervision and optimization of building`s electrical energy and power systems and Energy and Power reports
- Support of distributed systems expanding the limits of supported system objects to 750'000
- Support for validated environments and validated site reporting
- Extended support of different Building Automation, Fire and Security subsystems (see section 3.5 for details)
- Long term storage
- Increased openness with BACnet autodiscovery functionality, IEC61850 protocol integration and Schindler elevators
- Scripting
- In-graphics commands
- Extended support for Fire and Security
- Simplified UI for Fire Operators
- Full system documentation in the online help

# 1.1 Features and Benefits - What the System Does

## 1.1.1 Applications

### 1.1.1.1 Management Station for Building Automation

As a building automation management station, Desigo CC provides the full breadth of application support to ensure that facilities remain comfortable, productive, and achieve optimal energy and equipment performance.

The Desigo CC user interface coupled with easy operation and event workflows, openness and harmonized look and feel across disciplines and vendors makes Desigo CC the perfect tool for maintaining facility operation.

Desigo CC used as the management station for building automation systems allows users to:

- Graphically operate and monitor the building automation system and take control of HVAC equipment
- Take action by manually switching devices from auto to manual mode
- Detect, visualize, and acknowledge/reset faults and alarms
- Collect, visualize, and compare online and offline Trend data
- Create schedules to automate the operation of the building and set up exceptions, which override regular schedules
- Compose and configure report definitions to produce a variety of performance reports the building
- Store and retrieve system activity data, view data logs
- Create and execute automated reactions between the networked systems
- Send out automatic remote notifications via email, SMS, and pagers

### Alias

The Alias can be used to add site specific references to technical equipment or other facility infrastructure. The Desigo CC user interface supports customer specific naming concepts and displays names in a common manner across the integrated subsystems. The use of Alias may differ depending on the subsystem such as User Designation, User address, Vendor-specific-address, System Name, Structured Address, etc.

### Eco Monitoring

In combination with systems from Siemens that support the green leaf concept, Desigo CC offers real-time monitoring and reporting of the HVAC equipment performance from an economic and ecologic point of view. It displays the quality of operation with a green leaf in Graphics and identifies unnecessary energy consumption. It allows the user to optimize the operation in order to reduce energy consumption and wear and tear of components without affecting comfort in a negative manner.

### Flexible Room Management

When used with the Desigo system, Desigo CC allows the user to manage the office layout of a floor on demand. In Desigo CC's Flexible Room Management editor, rooms can be re-assigned to floor segments. In Addition, Central Function applications permit and support centralized control and coordination of defined groups, including a façade for blinds or multiple floors for lights. In Desigo CC the user can command, monitor or adjust elements of the Central Functions groups from a single vantage point.

### Support for Validated Environments

Desio CC has the ability to establish portions of a building automation system for Pharma and Life Sciences customers as compliant to regional certifications, such as US FDA 21CFR Part 11, GMP Annex 11 or similar

### Energy and Power Managment

Desigo CC offers an insight into electrical power distribution in a building and optimization of its operation. Supported by the “Managed Meters” and “Energy & Power Reports” features, it provides extensive coverage of power management applications in buildings and supports comprehensive and modular multi-discipline system offerings.

Optionally, Desigo CC collects and transmits trend series from metering devices to the Cloud based Energy Management service platform Advantage Navigator.

## 1.1.1.2 Management Station for Danger Management

As a danger management station, Desigo CC provides the full breadth of application support for ensuring life safety, property safety, and keeps facilities protected.

The Desigo CC user interface, coupled with event-oriented workflows, secured communication and approved fire norm conformance, make Desigo CC the perfect tool for Danger Management.

Desigo CC is designed for use with fire safety and security systems and allows users to:

- Visualize and handle events (for example, acknowledge, silence, and reset)
- Graphically monitor and control life safety and security systems
- Know where to start as the highest-priority events are highlighted
- Maintain continuous situational awareness of all fire panels with the graphical Node Map dashboard
- Directly navigate (with just one click) to the triggering element of an event
- Quickly navigate to custom operator instructions and graphical display of event locations
- Store and retrieve fire alarm system activity data
- Distribute fire, access, video and intrusion monitoring and control capabilities across a network of Desigo CC management clients
- Provide Operating Procedure checklists to guide the operator, under stressful conditions, in handling significant events
- Display multiple video streams
- Send out automatic remote notifications via email, SMS, and pagers
- Include and exclude (isolate/de-isolate) system devices
- View and schedule automatic history reports
- Provide “Ready To Arm” check for Intrusion

### Video Surveillance, Access Control and Intrusion

Security disciplines are integrated into Desigo CC to offer full coverage for a Danger Management System. Desigo CC harmonizes workflows, enriches information and adds specific applications for security for visual operation and monitoring, security management, or to visually confirm and document events that are displayed in the Event List.

### 1.1.1.3 Management Station for Mass Notification

In addition, Desigo CC offers an optional package for Mass Notification (MNS). The Mass Notification package uses audio, text, and multimedia to provide information and instructions to people who may be impacted by an emergency event, or other undesired situation, that may cause significant disruptions to people, interruption of services, property damage, personal injury or even death.

Desigo CC is designed for use with mass notification and allows users to:

- Centralize communication technologies from premise based to social media alerting, including bulk messaging
- Streamline activation methods to easily open and initiate an incident
- Pre-define or customize messages, edit on-the-fly; immediate or scheduled; targeted to specific zones, individuals, groups or devices with reply and escalation features for recipient users
- Search using Incident and notification browser for active and closed incidents and corresponding messages
- Keep recipients informed during emergency events via messages and live announcements

Possible notification recipients are SMS, Pager, IP Phones, E-mail, PC, LED signs, Media displays, Audio zones, Relay contact, CAP, Facebook, twitter and RSS feed.

Desigo CC Mass Notification major highlights

- **Easy buttons:** provide an easy and fast way for an operator to initiate incidents. The Easy Button bar is configurable according to customer needs.
- **One User Interface,** to monitor and control up to 16 different types of output channels.
- **Incident Wizard:** guides the operator through all the necessary steps for initiating an incident.
- **Powerful message Editor:** the Message Content (Text, Audio, Multimedia,…) Editor provides the operator with the capability to revisit predefined message details and make changes prior to their dissemination.
- **ACK:** Messages (Email, SMS) sent out can be acknowledged by the recipients. Recognizing the percentage of received messages, allows the operator to judge whether a resend is needed.
- **Recipients Import/Export Tool:** This import and export feature allows the customer to export all existing user accounts to the Desigo Mass Notification Recipients Database.
- **CAP** (Common Alerting Protocol) **Output:** The Desigo Mass Notifcation Web Feed Publisher CAP Output allows to forward incidents to other SW packages like e.g Rave Alert Emergency Notification.
- **CC Mobile app support:** Desigo **Mass Notification** V2.1 SR2 supports triggering incident templates from outside of the Desigo MN SW via REST Web services. E.g. this means, you may now trigger such MNS incidents via the Desigo CC Mobile App in addition to the already supported dial in possibility.
- **Repeat**: Repetition of Text, Audio or Multimedia content messages supported.
- **Safer configuration**: Filter defaults for incident trigger conditions have been changed, respectively restricted to avoid sending out simple fault messages to all recipients.

- ACK-Voice: Voice messages can be acknowledged by pressing a phone key. Depending on the reception of the acknowledgement it’s possible to escalate the notification to the same or other recipients

### 1.1.1.4 Management Station for multiple disciplines

As an integration platform, Desigo CC is designed for the simultaneous connection to multiple systems and use by multiple operators, each with their unique focus. Desigo CC assures the optimal system performance of building automation and danger management applications.

The workflow-oriented user interface provides the same look, feel and operation to all connected subsystems. This brings integration to the next level, a unification where tasks such as commanding, event handling, reporting, and scheduling are not differentiated by the subsystem.

The combined control and management of building automation and danger management disciplines on a single management system allow for interaction between those facilities.

Interaction examples:

- Unauthorized entry detected by the Intrusion system, initiates lighting and focuses the camera to the location.
- Deteriorating weather conditions, like a storm, cause sending a centralized command to the room systems, opening all blinds, and informing about window contact status.
- After successful access control authentication, access to the room is granted, Lights are activated and HVAC systems switched to occupied mode.
- Temporary noxious emissions, for example, from helicopter landing or vehicles at a loading dock, cause outside air dampers to close, stopping fresh air intake.
- Scheduled activation for entire building modes (for example, *night mode* sets lights off, blinds and HVAC plants to unoccupied mode, perimeter security, camera positions, lifts to base position).
- Under peak energy consumption conditions, inform the user and offer assisted procedure to optimize building equipment.
- Built-in applications for vertical transportation systems manufactured by Schindler Ltd. (for example, monitor elevator status, call a lift, treat passenger alarms and faults, lifts and escalator dynamic visualization).

## 1.1.2 Highlights

Desigo CC has been designed to be:

### Easy to learn and user-friendly

- Consistent interface designed around user-based workflows
- Simple navigation through tree views or graphics
- Auto-defined Links (so called Related Items) help anticipate the next step
- Graphics engine supports drag-and-drop and zoom
- Online engineering speeds-up project commissioning time and minimizes system downtime

### Optimal for maximizing operational and engineering efficiency

- Integrated data from multiple facilities, disciplines, and information systems

- Fast, Investigative, and Assisted Treatment for quick response to all kind of events
- Customized reporting capabilities
- Time-shifted trend graphs, Log Viewer, and Quick Search for data analysis
- Powerful multi-layered graphics supporting animated symbols, import of AutoCAD plans
- Built-in email, Pager and SMS for remote notification

### Adaptable to meet the needs of any facility

- Multiple client options for use at a dedicated workstation, in a browser, or as a light desktop application
- User groups and profiles control and simplify site visibility
- Built-in profiles for building automation, fire safety and security users
- Adjustable pane layouts support beginners and power users
- Separate Operation and Configuration modes
- Flexible Views allow users to organize facilities and to view them as they want

### Open, integrated system

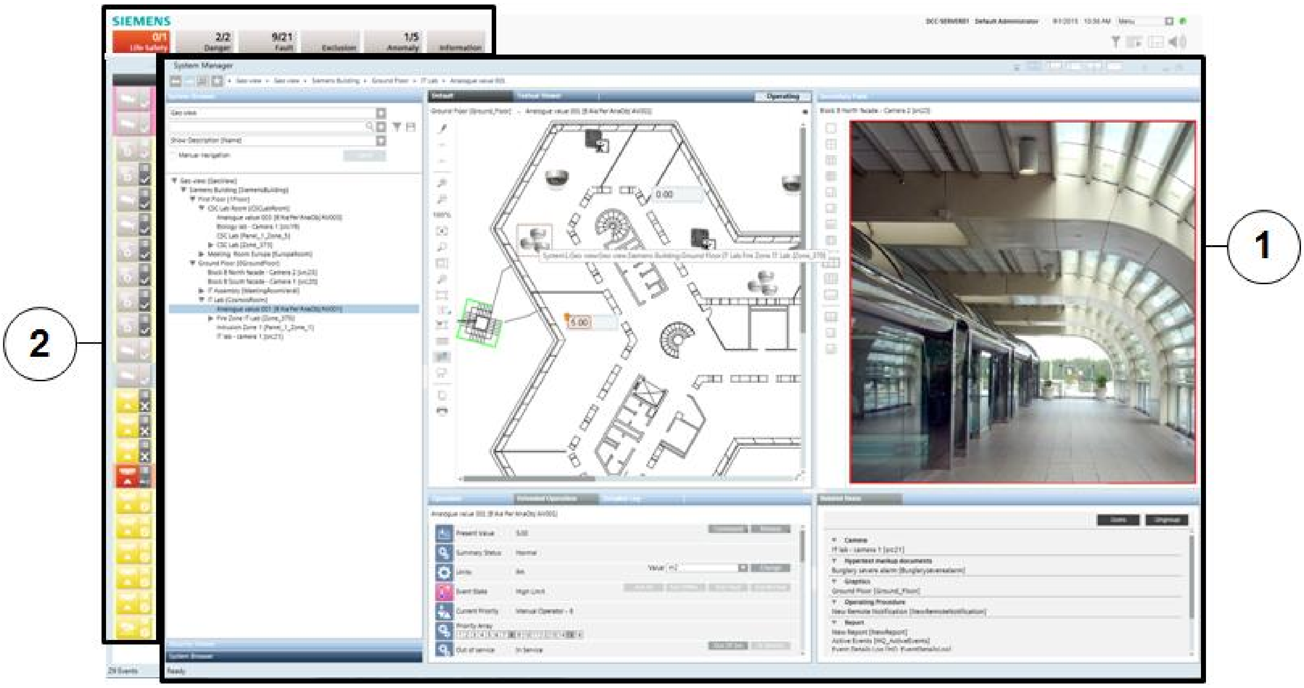
- Standard protocol support for building automation, fire safety and security systems
- IT compliant and IT environment enabled system
- Normalization and management of data from multiple sources
- Extended application development and support for simple and complex systems

### Robust System Platform

- Built on proven Siemens SIMATIC technology and IT standard components
- Scalable to support small and large facilities
- Flexible to provide a wide range of applications
- Highly secure client-server communication
- Extendable to grow with a facility’s needs

## 1.1.3 User Interface

Desigo CC’s User Interface provides effective system operation and control. It presents well arranged, relevant information to the user and is ready for interaction without any overlapping windows. The User Interface combines daily operation and event handling. The System Manager (1) is a multi-pane window for navigating, monitoring, and controlling all the components and subsystems of the site. Each pane contains a functional component of the management system (for example, a browser for navigating and selecting system objects, a viewer for displaying site floor plans, tools for scheduling tasks, and so on). Event Management (2) consists of a robust set of applications to ensure quick, easy, and accurate response to any event.

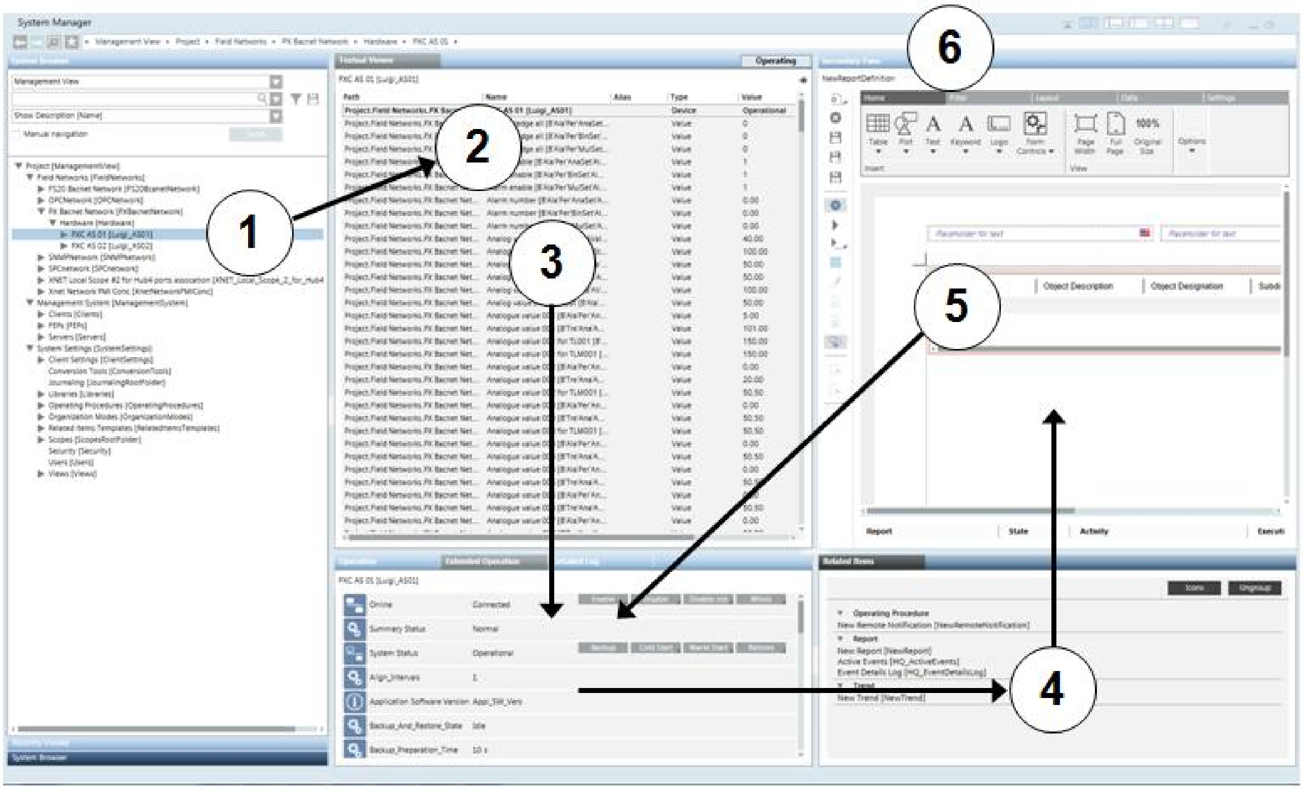


## 1.1.3.1 System Manager

The System Manager window is built around the concept of a common workflow for all system navigation. This simple and consistent workflow allows users to select from standard applications or for a more specific focus, select the part of the facility they are interested in and let the system guide them to the most relevant information.

From the initial starting point, users can make additional selections for more details, act on the system, or navigate further to automatically provided Links (Related Items) based on their selection. The pane-based navigation keeps important information in front of users with no overlapping windows. They can navigate the system through graphics or flexible views that allow the system to be represented in the way the users actually see their facility.

This image shows a typical navigation and operation workflow:



1) Perform a selection in *System Browser*

2) Get information and tools in the *Primary Pane*

3) Select and get more detailed information in the *Contextual Pane*

4) Access an additional menu in the *Related Items* pane

5) Get additional tools in the *Secondary Pane*

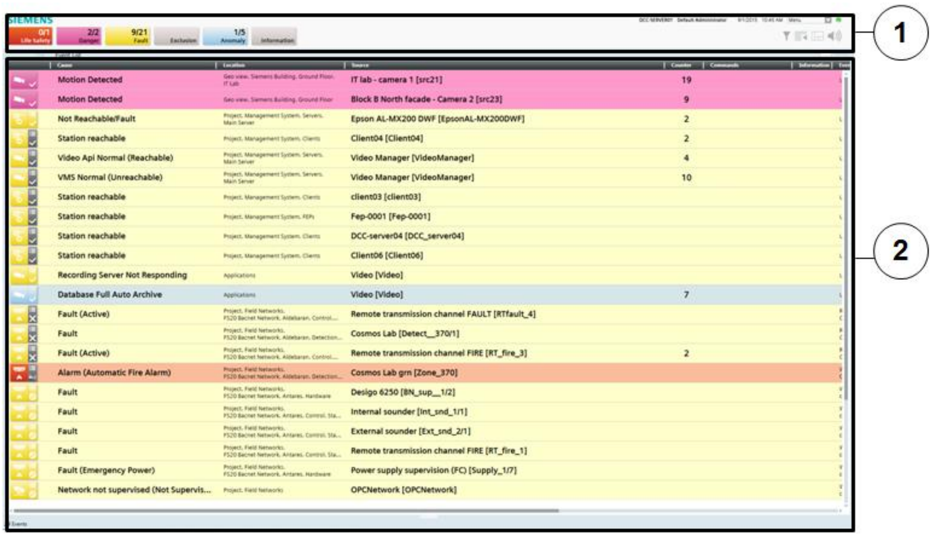
6) *Breadcrumb navigation on top of System Manager*

The paragraphs below describe the most important applications offered by Desigo CC for System Management.

### 1.1.3.2 Event Management

Event Management (also called event or alarm handling) refers to the various actions and steps that users take to respond to an event (e.g. smoke alarm) that occurs. Such actions may include, acknowledging the alarm, investigating its cause, resetting the alarm once the problem has been resolved, and filling out a report form.

The main applications provided for Event Management are the Summary bar (1) and Event List (2):



| Cause | Location | Source | Counter | Commands | Information |
|---|---|---|---|---|---|
| Motion Detected | Geo view, Siemens Building, Ground Floor, IT Lab | IT lab - camera 1 [src21] | 19 | | |
| Motion Detected | Geo view, Siemens Building, Ground Floor | Block B North facade - Camera 2 [src23] | 9 | | |
| Not Reachable/Fault | Project, Management System, Servers, Main Server | Epson AL-MX200 DWF [EpsonAL-MX200DWF] | 2 | | |
| Station reachable | Project, Management System, Clients | Client04 [Client04] | 2 | | |
| Video Api Normal (Reachable) | Project, Management System, Servers, Main Server | Video Manager [VideoManager] | 4 | | |
| VMS Normal (Unreachable) | Project, Management System, Servers, Main Server | Video Manager [VideoManager] | 10 | | |
| Station reachable | Project, Management System, Clients | client03 [client03] | | | |
| Station reachable | Project, Management System, FEPs | Fep-0001 [Fep-0001] | | | |
| Station reachable | Project, Management System, Clients | DCC-server04 [DCC_server04] | | | |
| Station reachable | Project, Management System, Clients | Client06 [Client06] | | | |
| Recording Server Not Responding | Applications | Video [Video] | | | |
| Database Full Auto Archive | Applications | Video [Video] | 7 | | |
| Fault (Active) | Project, Field Networks, FS20 Bacnet Network, Aldebaran, Control... | Remote transmission channel FAULT [RTfault_4] | | | |
| Fault | Project, Field Networks, FS20 Bacnet Network, Aldebaran, Detection... | Cosmos Lab [Detect__370/1] | | | |
| Fault (Active) | Project, Field Networks, FS20 Bacnet Network, Aldebaran, Control... | Remote transmission channel FIRE [RT_fire_3] | 2 | | |
| Alarm (Automatic Fire Alarm) | Project, Field Networks, FS20 Bacnet Network, Aldebaran, Detection... | Cosmos Lab grn [Zone_370] | | | |
| Fault | Project, Field Networks, FS20 Bacnet Network, Antares, Hardware | Desigo 6250 [BN_sup__1/2] | | | |
| Fault | Project, Field Networks, FS20 Bacnet Network, Antares, Control, Sta... | Internal sounder [Int_snd_1/1] | | | |
| Fault | Project, Field Networks, FS20 Bacnet Network, Antares, Control, Sta... | External sounder [Ext_snd_2/1] | | | |
| Fault | Project, Field Networks, FS20 Bacnet Network, Antares, Control, Sta... | Remote transmission channel FIRE [RT_fire_1] | | | |
| Fault (Emergency Power) | Project, Field Networks, FS20 Bacnet Network, Antares, Hardware | Power supply supervision (FC) [Supply_1/7] | | | |
| Network not supervised (Not Supervis... | Project, Field Networks | OPCNetwork [OPCNetwork] | | | |

## Summary Bar

The Summary bar is the anchor for Desigo CC event management. It highlights current conditions with a clear indication of current event priorities, and allows the user to quickly open the Event List. Depending on the client profile in use, the Summary bar can be docked on the desktop or freely opened and closed as needed. In some configurations, the one or two most important alarms are also displayed in an Event Detail bar underneath the Summary bar.

## Event List

The Event List application provides a complete and easily filtered list of events under control of the management station. When expanded, the Event List provides a clear indication of each event source, severity, and current status, as well as custom messages and suggested steps through the use of text, color, and icon representations. Events can be acknowledged, silenced, and reset from the Event List.

To handle an event Desigo CC offers the following alarm-handling options:

## Fast Treatment

From the Event List or Event bar, operators can quickly select an event and perform all the commands (for example, Acknowledge, Reset, Close, or Suspend) from the Event Detail bar and Event List, without following any advanced guided procedure (such as, viewing live and recorded video streams or a map of the alarmed area, and so on). A brief description of the next action to take (which command to select) is also contained in the event descriptor (the event descriptor is visible when the Event List is expanded).

When event handling is in progress, the user can send the available commands to the source object causing the event or even suspend event handling.

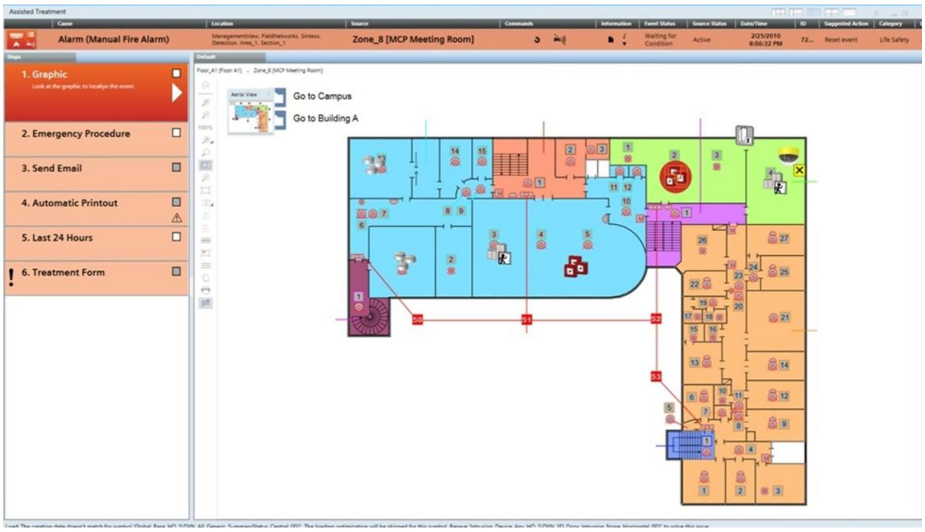
## Investigative Treatment

From Event List or the Event bar, operators can quickly open System Manager with a focus on the source of the event, and all information (live and recorded video streams, recent history, schedules, and so on.) related to the event source.

## Assisted Treatment with Operating Procedures

Operating Procedures consist of a sequence of steps or actions, which the operator must, or is suggested to perform with Assisted Treatment. The system provides instructions and operating tools on each step of a procedure. With appropriate permissions, a user can create, view, edit, or delete Operating Procedures.

From Event List or the Event bar, operators can quickly open Assisted Treatment to guide the operator through pre-configured Operating Procedures. Each Operating Procedure is composed of steps - some of which may be mandatory - for the user to complete (for example, view the graphic of the object in alarm, view live and recorded video streams, or complete an event handling form) while other can be configured to be executed automatically by the system (for example, sending emails to recipients or printing the even information).



Assisted Treatment

| Cause | Location | Source | Commands | Information | Event Status | Source Status | Date/Time | ID | Suggested Action | Category |
|---|---|---|---|---|---|---|---|---|---|---|
| Alarm (Manual Fire Alarm) | ManagementView. FieldNetworks. Sinteso. Detection. Area_1. Section_1 | Zone_8 [MCP Meeting Room] | | | Waiting for Condition | Active | 2/25/2010 8:06:32 PM | 72... | Reset event | Life Safety |

Steps

1. Graphic □ Look at the graphic to localye the event
2. Emergency Procedure □
3. Send Email □
4. Automatic Printout □ ⚠
5. Last 24 Hours □
6. Treatment Form □ !

Detail

Floor_A1 [Floor A1] › Zone_8 [MCP Meeting Room]

## 1.1.4 Main features

### Graphics

Desigo CC graphics are built using smart objects that know how they are used and how to represent themselves graphically. The use of smart objects allows users to create graphics by simply dragging-and-dropping objects onto a page, without manually binding an object to graphical symbols. Any system object can be commanded via Graphics with one click.

The Graphic editor also provides a powerful AutoCAD importing tool that allows the user to select and manipulate layers of AutoCAD drawings both during and after the import process.

Standardized graphic libraries increasing the engineering efficiency and provide a distinctive design. Library elements can be customized to the particular project.

### Textual Viewer

The Textual Viewer provides a quick summary of the current value and status of any selected object without any prior system configuration. This is a handy tool for getting an overview of system status.

### Trend Viewer

Both panel-based and workstation-based trending is provided to support control systems without embedded Trend capabilities.

Trend data is stored in a Microsoft SQL Server database. SQL Server Express is included with the Desigo CC software, and can be upgraded as required.

The Trend Comparison View allows users to time shift the Trend View to compare data at different times for quick analysis of changing conditions.

## Long Term Storage and archiving

Desigo CC now allows you to maintain extensive amount of historic data on line, also providing support for on-line data archiving and on-demand re-mounting.

## Schedules

The scheduling application allows complete configuration and display of standard BACnet schedule, calendar, and command objects, as well as for workstation-based schedules that can be used to support subsystems without built-in scheduling capabilities.

Schedules are automatically associated to the systems they control, so users can quickly navigate to the schedules related to any selected object.

The Timeline Viewer in the scheduler application allows users to show the details of multiple workstation schedules or field panel schedules simultaneously, spanning a range of time.

## Macros

Macros are predefined lists of commands that enable a user to send out a group of commands to specified devices with a single action. Some macros can be started manually while others may be part of schedules defined for time-based functions or automatic reactions.

Macros are also used by the system to perform multiple command actions. These predefined system macros are applied to specific control actions, such as block commands to fire control panels and system backup functions.

## Reaction Processor

The Reaction Processor allows the user to configure Desigo CC to automatically execute given actions when some conditions are verified. Conditions can be based on time (for example, every Monday at 7:00 AM), on events (for example, when technical equipment is in fault), on change of values (for example, when the temperature of a room is higher than a predefined value), or on a combination of some or all of the above. When conditions are met, the Reaction Processor executes a pre-configured list of commands (for example, switch on the lights).

## Scripting

Desigo CC provides a Script Editor to create sophisticated and powerful script programs based on Javascript language. Scripts can be executed on demand or automatically by the system based on trigger conditions.

## Reports

The Desigo CC reporting tool includes standard reporting templates (for example Status, Event or Configuration templates) and allows a user to create fully configurable reports with custom logos, headers, footers, and layouts that include tabular and graphical system information. Reports can be scheduled, and saved in CSV or PDF formats for future use and/or programmed to be sent via email to pre-configured recipients (for example, every Monday morning at 8.00 AM, a report with all alarms occurred over the previous seven days is created and sent to the Facility Manager).

## Log Viewer

The Log Viewer application provides a historic log of user and system events and activities that have occurred. It allows users to retrieve these historic events and activities for further analysis and investigation.

The Detailed Log within the Contextual Pane provides a historic log of the most recent user and system events and activities related to an individually selected object. For example the system logs user intervention to set point with previous, new value, timestamp and username. Data displayed within the Detailed Log can be further analyzed using sorting and filtering functionality similar to that of the Log Viewer.

### Document Viewer

The Document Viewer displays object-related data sheets, operating manuals or other information contained in a document file (for example: a data sheet for a detector or sensor) or web page.

### Remote Notification

Desigo CC can be configured to automatically or manually send email, pager or SMS messages to first responders in case of alarm. In addition to simple notification, notification can also be escalated to second level responders as needed.

### Mobile App

Desigo CC app lets an operator view and handle the alarms and objects of the integrated building management platform Desigo CC. Mobile App connects via Desigo CC Web Services and consume Web Service sessions.

### Video Surveillance

With Video Surveillance, the user can monitor and operate video streams, video devices including cameras and monitors and the video recording archive. Typical live view operations are supported, including live video streams, camera groups and sequences, PTZ and preset operations as well as recording and replay operations such as recording commands, tagging and recording bookmarks and search and replay of video recordings.

## 1.1.5 Online Engineering

Desigo CC makes the engineering of the system easy and fast as it comes with an innovative online engineering concept. A user can toggle the system to *Engineering mode,* where system parameters can be set up and user accounts managed.

The benefits of such functionality is that any type of configuration changes can be done online without the need to start external tools and, finally, download the updated configuration to the online system. This method significantly reduces engineering time as well as the system downtimes (while waiting for the new configuration to apply).

## 1.1.6 Library Concept

Desigo CC provides an extremely powerful and flexible library concept that allows, on the one hand standardization of system operation, and on the other a further drastic reduction of engineering time.

Libraries that are made available with the product distribution provide extensive coverage of Building Automation, Fire and Security, including specific applications such as Data Centers and Life Science.

In addition, Desigo CC libraries can be extended at any time on site, to cover project or domain specific applications.

The Library concept contributes to system openness, as it makes it possible to full integrate subsystems communicating via standard protocols.

## 1.1.7 Multilanguage Support

Desigo CC is a multilingual system that offers the ability to support, in the same project configuration, multiple languages. The Desigo CC client application is in fact able to displays project data, as well as user interface texts in the language of the user who is logging on the system.

è For a detailed list of supported languages please refer to the *Supported Languages* section on p.66.

## 1.1.8 Connectivity

Desigo CC is able to integrate and communicate with a wide range of product families from Building Automation to Fire Safety and Security systems.

### Building Automation

- APOGEE
- Climatix
- Desigo
- SIMATIC S7
- SICLIMAT X engineered S7 PLC

### Fire Safety

- Algorex
- Desigo Fire Safety FS20 UL
- Desigo Fire Safety Modular
- FireFinder XLS and MXL
- Sinteso FS20 DE/EN

### Security

- Milestone XProtect Expert/Corporate
- Sintony
- SiPass integrated
- Siveillance VMS
- SPC Intrusion

### Mass Notification

Mass Notification Sub systems, approximately 30 different notification devices available, see the MNS Online Help.

è For more details on supported systems please refer to the *Supported Subsystems and Standard Field Network Protocols Compatibility* section on p. 64.

## 1.1.9 Open Platform

Desigo CC is an open platform by design and supports a variety of standard protocols and interfaces for field network integrations. Furthermore Desigo CC can provide data to external applications and services.

### 1.1.9.1 Standard Protocols

Desigo CC communicates with field network devices to monitor and command information by using the following standard protocols:

- BACnet
- OPC DA (Data Access)
- Modbus TCP
- SNMP
- ONVIF
- IEC 61850

è For more details on supported protocols please refer to the *Supported Subsystems and Standard Field Network Protocols Compatibility* section on p. 64.

In addition, the connected systems offer a large selection of proprietary and standard protocols, such as DALI, EIB/KNX, LON, M-Bus, Modbus RTU and so on.

### 1.1.9.2 Subsystem integration with SORIS

SORIS stands for Southbound Open RESTful Integration Service. It provides an open integration framework for Desigo CC that is easy to work with interoperability between computer systems on the internet: Developers can use the SORIS SDK to create SORIS adapters in Java or C# that map to the foreign system’s protocol or interface. For security reasons, stage 1 adapters should be deployed locally on the Desigo CC server or FEPs. They can be deployed on other Windows, Linux or embedded device hosts inside the intranet via secure https communication and a VPN.

### 1.1.9.3 Web Services with NORIS

NORIS stands for Northbound Open RESTful Integration Service. Desigo CC allows external applications to read and write real time data as well as access events or historical values, by using the provided REST (Representational State Transfer) web service interfaces, e.g. NORIS. Web Services can be used for applications such as Enterprise Software, Energy Management services, Facility Management systems or Mobile Apps.

### 1.1.9.4 OPC Server

Desigo CC allows Enterprise Applications or other Management Systems to access real time values from integrated subsystems via OPC. The Desigo CC OPC Server supports the OPC DA (Data Access) specification. In addition an OPC UA wrapper provides OPC UA Clients access to the exposed data.

## 1.1.10 Certifications and Approvals

Desigo CC has been tested against a wide range of domain and country-specific norms and standards, including:

- BACnet Revision 1.13, certified by BACnet Testing Laboratory as BACnet Advanced Workstation Software (BTL B-AWS)
- AMEV recommendation BACnet 2011 compliant with Management Operation Unit (MOU-B) profile
- IT security compliant with the ISA-99/IEC 62443 Security Level: SL1

- OPC DA V2.05a and V3.0 Server, certified by the OPC Foundation certification program
- UL listed to UL864 9th edition *Standard for Control Units and Accessories for command and control* when installed on a UL864 approved computer
- ULC listed to ULC-S527-11 3rd edition for command and control when installed on a ULC-S527 approved computer
- UL listed to UL2572 for Mass Notification (for monitoring only when installed on a UL2572 approved computer)
- ULC listed to ULC-S576 for Mass Notification (for monitoring only when installed on a UL2572 approved computer)
- Support of pharmaceutical industry regulatory requirements, such as US FDA 21CFR Part 11, GMP Annex 11 or similar

**NOTE:**
UL-294 requirements are not supported. Because that Desigo CC cannot be connected to a Fire System and an Access Control system at the same time, meaning in the same Desigo CC system, maintaining UL-864 approval.

**NOTE:**
Desigo CC has no negative feedback on connected fire detection units like FS20 and Algorex.

# 1.2 System Architecture - How the System is Organized

Desigo CC is a client/server system designed to augment existing building infrastructure and integrate with standard IT hardware, software, and networks. The open and adaptable architecture supports the most common Windows-based IT infrastructures. In addition, Desigo CC allows full server functionality in customer’s virtual IT environments and advanced networks. Desigo CC deployments are tested using state-of-the-art firewalls and network configurations such as IPv6 as well as domain configurations and standard software, i.e. virus scan and malware protection software.
This allows large enterprises and small businesses alike to use Desigo CC in their existing IT environment to manage a building’s infrastructure. The support of remote services such as history databases, Web Server, Windows App and Web Clients offer a broad variability of deployments to meet project requirements.

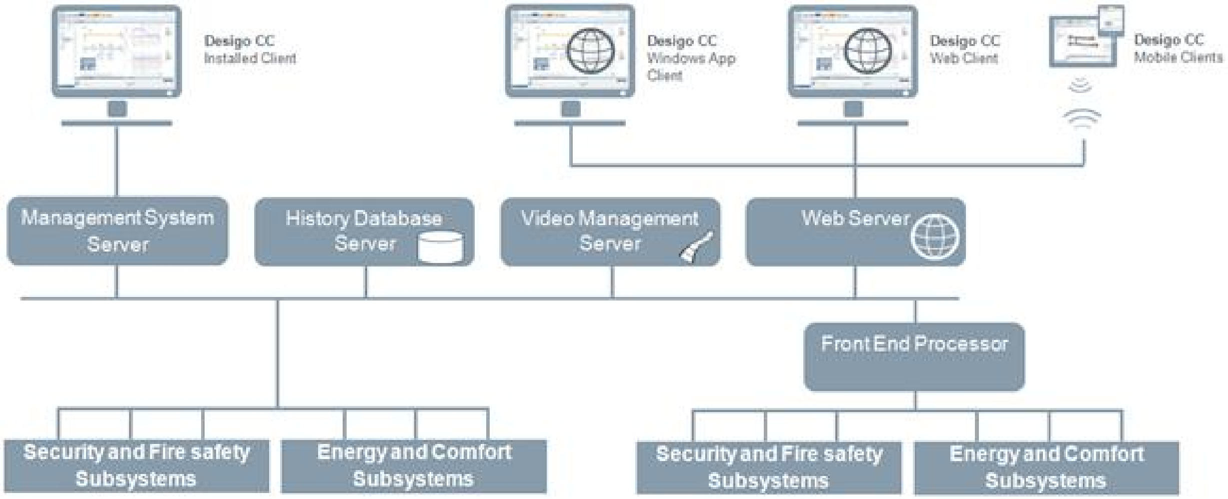
è Refer to the *Typical System Deployments* section on p.30

## 1.2.1 System Components

As illustrated below, Desigo CC software can be installed on a single server or broken up in the following main functional blocks:

- Management System Server: Monitors and commands the field networks, executes automatic actions and interacts with users via clients.
- Database Server: Manages the Historical data collected by Desigo CC
- MNS
- Video
- Web Server: provides connectivity for Web Clients
- FEP (Front End Processor): Extends and distributes connectivity to field networks

- Installed Clients: Provide user access to Desigo CC user functionalities, connecting directly to the Management System Server
- Windows App and Web Clients: Provide user access to Desigo CC functionalities via Web Server.


Desigo CC Installed Client
Desigo CC Windows App Client
Desigo CC Web Client
Desigo CC Mobile Clients
Management System Server
History Database Server
Video Management Server
Web Server
Front End Processor
Security and Fire safety Subsystems
Energy and Comfort Subsystems
Security and Fire safety Subsystems
Energy and Comfort Subsystems

### 1.2.1.1 Management System Server

The management server is the main component of Desigo CC. The Desigo CC Server installation always includes an Installed Client and a System Management Console (SMC) that provides the user interface to configure and administer the system and host field system drivers. The server hosts the project to monitor and control the facility including runtime data. Projects are managed by the System Management Console. The administrative operations required to activate a project with all necessary information are also supported.

The System Management Console is a stand-alone tool that initializes a new project, restores a project, and configures system-wide settings such as history database, system users and web server parameters.

The Desigo CC project contains all engineering and operation information created for a system. Field system information is described by Desigo CC objects inside the project. Objects can be created manually, imported through data exchange files, or uploaded through a selective auto-discovery mechanism depending on the type of system being connected.

A unique, extensible object modeling approach allows Desigo CC to normalize information brought in through any interface and to provide the same look, feel, and operation through a common set of applications regardless of the source of the data.

The Management System Server contains an image of the field network systems, which are modeled as objects. Technology limits the total number of objects a System Manager can host. In the current Desigo CC version, the limit is set to 150,000 objects and 450,000 objects for a physical server working on a distributed system in a segmented configuration. See page 33.

The actual number of objects that can be hosted might be further limited by hardware resources (please refer to the Hardware Category Definitions section on p. 67).

### 1.2.1.2 Web Server

Web servers allow a web browser to access the system on the customer's intranet or the Internet. A web server is required to use the Desigo CC Web and Windows App Clients or the Web Services.

Desigo CC Web Server is based on Microsoft Internet Information Services (IIS). IIS needs to be installed on each computer serving as the web server. IIS installations on remote computers are supported, such as in demilitarized zone (DMZ).

A web server can be installed on the same hardware running the Management System Server or on a separate, dedicated computer.
The latter applies for instance, if the customer’s IT department requires using existing web servers, to be installed in a separate controlled environment, or if it is preferred not to use the resources of the system server for IIS.

By accessing a system web page in the Microsoft Internet Explorer, all files required for Web Clients, Windows App Client environments and the system documentation can be downloaded.

### 1.2.1.3 Front End Processor (FEP)

The Desigo CC Front End Processor is an extension to the Desigo CC Server to provide additional resources to connect subsystems. Additionally, FEP can be used as a bridge to connect an IIS to Desigo CC.

Running on separate hardware, FEP allows load balancing by distributing field system drivers across multiple machines. Additionally, FEP can be used to facilitate data exchange for distributed subsystems.

The Desigo CC FEP installation always includes an Installed Client and a System Management Console.

### 1.2.1.4 Historic Database Infrastructure

#### History Database

Desigo CC History Database Server manages historical data collected from subsystems and user activities. The Server uses Microsoft SQL to store, manage and maintain the historic data of the system.

The Desigo CC Database Service runs on the Desigo CC Server and connects to a Microsoft SQL Server hosting the History Database (HDB).

HDB is used to log a wide range of records including:

- User and system activities, e.g. user log-in an log-outs, access to applications, monitored clients connections, system restarts etc.
- Events, like alarms and faults and their guided procedure steps.
- Field network activity such as, change of states, change of values, commands
- Trends and time series.

è For details about the range of logged user activities and system events, please refer to the *Reports* section of the *Desigo CC User Guide.*

#### MNS Database

Desigo CC Mass Notification Database may run as a separate DB on the same SQL Server DB as the HDB and stores the MNS application data with the following main entities:

- Recipients
- Incident Templates

- Notification Templates

### Databases setup

To reduce the load on the main server, Microsoft SQL Server can be installed on a separate machine or in a virtual environment. Desigo CC can also use existing customer provided Microsoft SQL infrastructure.

Microsoft SQL Express is included on the product installation. If the system requirements exceed the capacity of Microsoft SQL Express, Microsoft SQL Server regular editions can be used, extending storage capacity and increasing the performances of the history database operations. Procuring and installing Microsoft SQL Server regular editions is not part of the Desigo CC offering. The software licensing, administration, and maintenance of Microsoft SQL Server regular editions is the responsibility of the customer.

## Long Term Storage and Archiving

The History Database supports four standard archive groups, related to the record types for events, value changes, activity and trends. All system objects are storing their data in the specific archive group depending on the type of record. Data of the standard archive groups are stored in “ring buffer” tables, meaning that, after a configurable retention time, the overflow data is deleted to allow space for the new data.

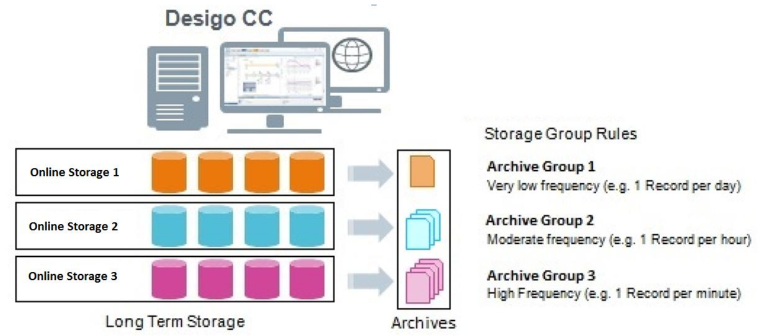
With Long Term Storage the basic capability of the historic database infrastructure is extended.

On top of the ring buffer tables, it is possible to configure multiple on-line stores. An on-line store is a set of data-slices of configurable size or duration. Data is stored in a slice as long as the size or duration limits are met, then passing to the subsequent slice. When the maximum number of configured slices is reached, the data of the oldest slice is archived off line. Offline archives can be remounted on demand when old data needs to be available online for access from a Desigo CC application.

This mechanism allows maintaining extensive amounts of historic data on line, providing as well support for on-line data archiving and on-demand re-mounting.

Moreover, besides the standard archiving groups, Long Term Storage allows to define custom archive groups.
A custom archive group allows assigning a specific subset of system objects and record types to a specific store.

This feature is particularly useful when events, value changes, activity or trends information for a part of the system require different retention times or simply need to be segregated due to, for example, the nature of data, special regulations, specific discipline demands or different on-line persistence needs.



NOTES:

**Estimate the Database size for HDB to Determine the SQL Server Edition**
The amount of collected historical data and the storage of the data to the HDB is highly specific to the particular conditions. The *Dimensioning Calculator Tool* (p. 41) provides indications about the edition and the database size most suitable for a specific project.
Please see section *History Database* in the *Desigo CC User Guide* for details on how to size the HDB and determine the adequate SQL Server edition.

**System Limits**
There is a 10 GB limit to the SQL Server Express database, and of 250 GB for SQL Server.

### 1.2.1.5 Video Service

The Desigo CC Video Service runs on Desigo CC Server and connects either to the embedded Video Management Service or to an external Video Management System (VMS).

The embedded Video Management Service provides the capabilities of a Video Surveillance System inside Desigo CC. The Video Management Service can be installed on the main server or on a separate machine.

For small systems, an additional Network Video Recorders (NVR) service can be installed on the main server. To reduce the bandwidth demands of the network and the required resources on the server, further NVR services can be distributed on other machines and storage devices.External Video Management Systems provide their own service architecture.

è For additional details, please refer to the engineering manual of the external VMS.

**NOTE:**
Only one Video Service is allowed in a distributed system configuration.

### 1.2.1.6 Client Options

Desigo CC supports multiple client options for applications ranging from occasional users to dedicated mission-critical console installations. All client options are built around the same usability standards and capabilities making it easy to switch between different client options without the need to learn multiple interfaces.

User privileges can be assigned to users and to workstations, allowing users to be granted the same access from everywhere or different access depending on where they are logged on.

#### Windows App Client

The Desigo CC Windows App Client software is a light application that can be downloaded from the Desigo CC Server through a browser. When the Windows App Client is downloaded, it runs like any other Microsoft Windows desktop applications. The Windows App Client is not installed but instead run by the Microsoft .NET runtime environment. It can be launched from the **Start** menu, from a desktop icon, or from the **Quick Launch** toolbar. This deployment does not require administrative privileges.

Depending on the configuration, Windows App Clients can have the same functionality as Installed Clients (Identified by certificate) or are restricted by other access mechanisms (anonymous client).

Each time the user launches Desigo CC as Windows App Client, a search for system updates is performed. If a new version of the system is available on the web server, the user can choose to update it or continue to use the current version.

Windows App Clients require low latency and low network bandwidth and are appropriate for Branch Office and Home Office connectivity. Internet use is supported but requires substantial IT Security measures.

**NOTE:**
Closed mode is not available on Web and Windows App Clients!
Regulations (such as, UL/ULC) restricts the use of current Web and Windows App Clients.

### Web Client (Browser Client)

This client option is deployed on the intranet with full trust and requires access to local machines. The system runs in Microsoft Internet Explorer 11 (using https as communication protocol) and is downloaded on demand each time the user launches the client as a web application. When working in a browser, the user can have the same functionality available as those working on an Installed Client or it can be restricted to have a different access when connected remotely. Web Clients do not support Closed Mode.

Web Clients require low latency and high network bandwidth and are appropriate for intranet connectivity. Internet use is supported but operators have to accept a degradation of performance and require substantial IT Security measures.

### Installed Client

The Installed Client is designed for mission-critical applications, such as fire safety monitoring or critical process control, where users are focused entirely on monitoring and managing building systems. In this configuration, UI components used for Event Management are locked in place and cannot be moved or covered by other applications; this ensures that critical events are never missed or hidden. Additionally, they can be monitored from the outside by the computer monitoring hardware (Comark cards).

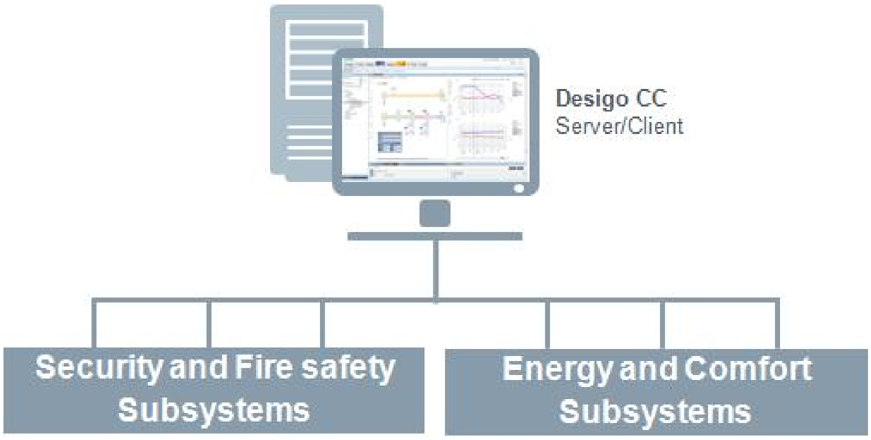
Installed Clients can optionally be configured to run in Closed Mode where only Desigo CC and other specifically identified applications are allowed to run. In Closed Mode, the workstation is dedicated to running Desigo CC, with access to the Start menu or other operating system and customer applications available only to administrative users.

## 1.2.2 Typical System Deployments

The key components of Desigo CC can be deployed in different configurations to optimally satisfy the requirements of the customer project. Examples of deployments are provided below.

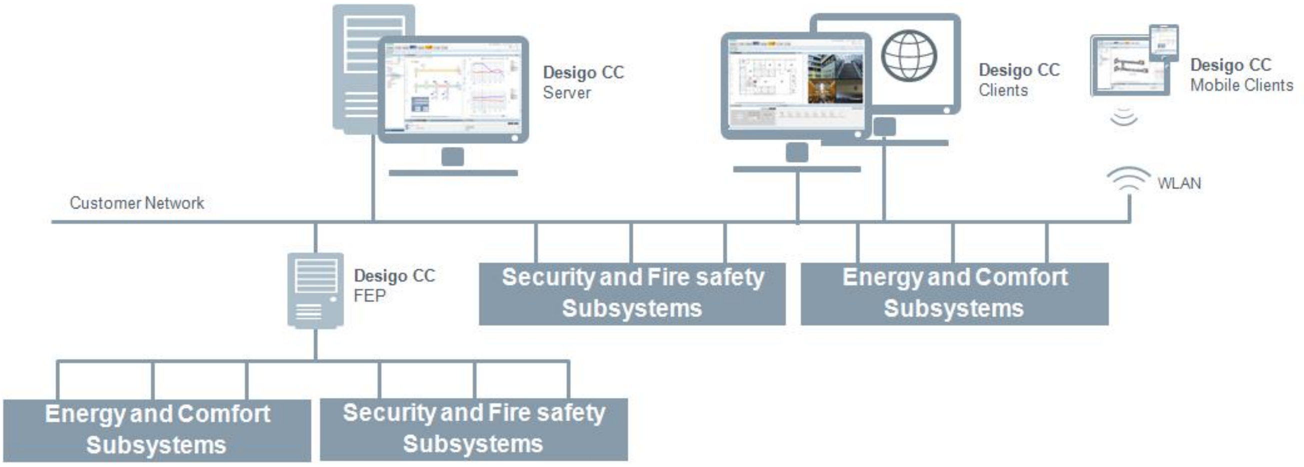
### 1.2.2.1 All-In-One (One-Seat) System

This is the configuration choice in all cases where only one client is required and system size is limited. Management System Server, database service and one installed client are deployed on the same hardware platform, which can be physical or virtual. The field networks are connected directly to the Management System Server.


Desigo CC
Server/Client
Security and Fire safety Subsystems
Energy and Comfort Subsystems

### 1.2.2.2 Client/Server inside the Customer Network

This is the configuration choice for the cases where multiple Installed Clients, connected via a dedicated or shared local area network (LAN) are required. Web connectivity is not required. Communication between the key components can be secured by standard IT security mechanisms like certificates.


Desigo CC Server
Desigo CC Clients
Desigo CC Mobile Clients
WLAN
Customer Network
Desigo CC FEP
Security and Fire safety Subsystems
Energy and Comfort Subsystems
Energy and Comfort Subsystems
Security and Fire safety Subsystems

The Management System Server, database service and the first installed client are deployed on the same hardware platform, which can be physical or virtual. If Windows App Clients are required, the Web Server can also be installed on the same platform.

Field networks are connected directly to the Management System Server.

FEP can be used to better balance the communication load or to better adapt to the distribution of the field systems. A typical case for FEP usage would be a system with multiple remote sites and one central control location.

Installed and Windows App Clients are connected via the system LAN to the server.

The size of the field system and the number of clients that can be supported by this configuration depend on the server hardware configuration.

è Please refer to Part B: System Dimensioning Guidelines on p.41.

### 1.2.2.3 Client/Server with Internet Access

This is the configuration choice for the cases where multiple Installed Clients, connected via a dedicated or shared LAN are required, but web connectivity is also required to allow remote access via a Desigo CC Web Client or provide remote connectivity to an external application via Web Services.
The Management System Server, history database service, Web Server and the first Installed Client are deployed on the same hardware platform, which can be physical or virtual.

Field networks are connected directly to the Management System Server.

FEP can be used to better balance the communication load or to better adapt to the distribution of the field systems. A typical case for FEP usage would be a system with multiple remote sites and one central control location.

Installed and Windows App Clients are connected via the system LAN to the server.

The size of the field system and the number of clients that can be supported by this configuration depend on the server hardware configuration.

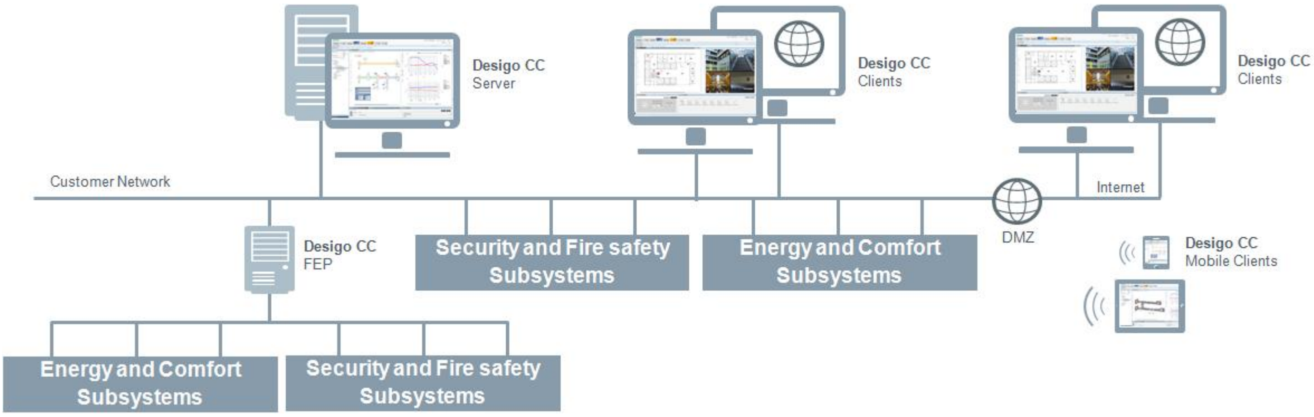
è Please refer to Part B: System Dimensioning Guidelines on p.41.

For systems with Internet access additional support for networks and IT security is available:

- Support of Windows domains and Active Directory
- Support of network policies
- Firewall/DMZ support

For systems with key components in the Internet additional network and IT security measures need to be implemented to run Desigo CC properly:

- Only Web and Windows App Clients are hosted outside the customer network
- Communication between all key components is required to be secured by standard IT security mechanisms like virtual private network (VPN) and/or certificates
- Communication to components in the Internet must be secured by customer or trust center provided certificates and separated from the customer network by professional hardware firewalls/DMZ
- Logon to Desigo CC in the Internet only with users of the customer Active Directory
- Field systems must be separated from Internet access


Desigo CC Server
Desigo CC Clients
Desigo CC Clients
Customer Network
Internet
DMZ
Desigo CC FEP
Security and Fire safety Subsystems
Energy and Comfort Subsystems
Desigo CC Mobile Clients
Energy and Comfort Subsystems
Security and Fire safety Subsystems

### 1.2.2.4 Large, Distributed Client/Server with Internet Access

This is the configuration choice for cases where system size or specific customer indications require the deployment of key Desigo CC components on different hardware platforms, which can be physical or virtual.

Communication between the key components is required to be secured by standard IT security mechanisms like certificates. Communication to components in the Internet must be secured by customer or trust center provided certificates and protected by professional hardware firewalls/DMZ.

Field networks are connected to the Management System Server, and when appropriate FEP can be used.

The size of the field system and the number of clients that can be supported by this configuration depend on the server hardware configuration.

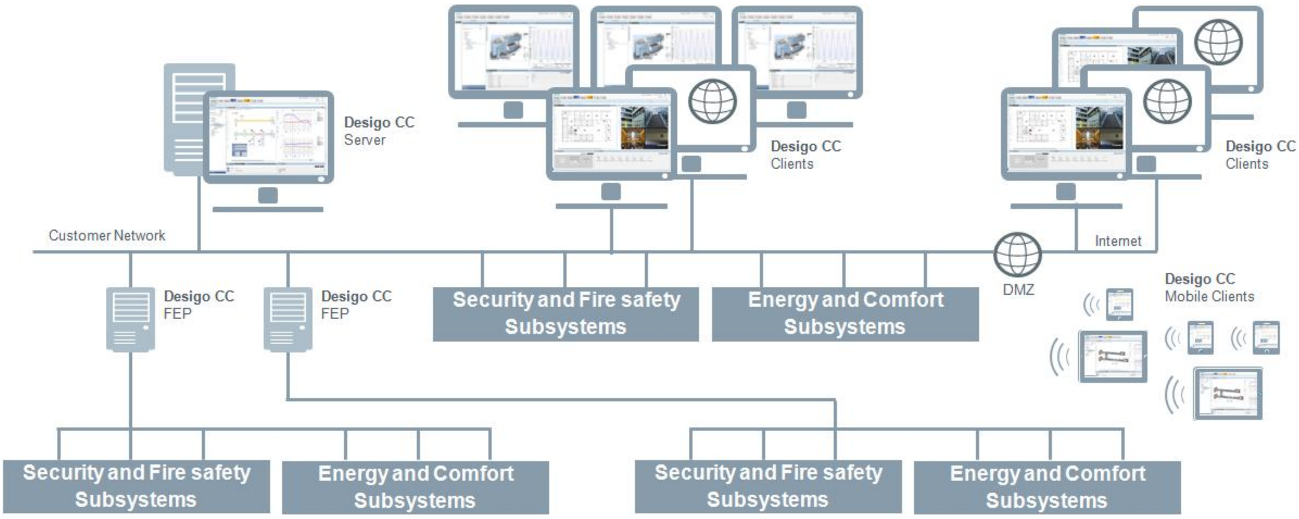
è Please refer to Part B: System Dimensioning Guidelines on p.41.

For systems with Internet access additional support for networks and IT security is available:

- Support of Windows domains and Active Directory
- Support of network policies
- Firewall/DMZ support

For systems with key components in the Internet additional network and IT security measures need to be implemented to run Desigo CC properly:

- Only Web and Windows App Clients are hosted outside the customer network
- Communication between all key components is required to be secured by standard IT security mechanisms such as VPN and/or certificates
- Communication to components on the Internet must be secured by customer or trust center provided certificates and separated from the customer network by professional hardware firewalls/DMZ
- Logon to Desigo CC on the Internet only with users on the customer's Active Directory
- Field systems must be separated from Internet access

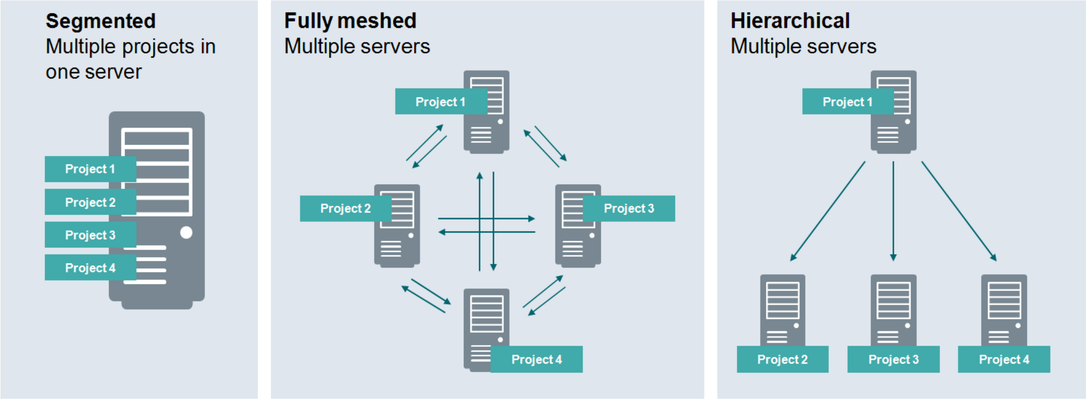

Desigo CC Server
Desigo CC Clients
Desigo CC Clients
Customer Network
Internet
DMZ
Desigo CC FEP
Desigo CC FEP
Security and Fire safety Subsystems
Energy and Comfort Subsystems
Desigo CC Mobile Clients
Security and Fire safety Subsystems
Energy and Comfort Subsystems
Security and Fire safety Subsystems
Energy and Comfort Subsystems

## 1.2.2.5 Distributed System Configurations

The distributed system configuration allows interconnecting several projects that run independently, either on one or several physical machines. The interconnection of the projects allows transparent engineering and operation through them seeing them as one only system. The distributed system configurations extends even further the support of very large systems, increase robustness eliminating single point of failures and allow geographical or discipline segregation.

Three types of distributed deployments are supported:

- Fully meshed: Each server is logically connected to all others. Clients can see all objects in all servers. Servers can be geographically distributed. Virtual servers are also supported.
- Segmented: A fully meshed configuration where all systems run on the same server. Allows to build larger systems on one single server
- Hierarchical: front servers are logically connected to one head server. Clients connected to the head server can see all objects; clients connected to front servers can only see local objects. For campus or inherently hierarchical applications



## 1.2.3 Virtualization

Virtualization has become a widely preferred and suggested environment for IT infrastructure by IT administrators:

- Server (Hardware) Virtualization is a proven software technology that makes it possible to run multiple operating systems on the same server at the same time, sharing the available hardware resources. It simulates the available hardware and deludes every operating system running on top of it to assume that it is the unique holder of the resource. The details of the physical environment are kept transparent from the operating system.
- Add-On options for hardware redundancy allow running the same virtual machine on multiple physical servers. If a server fails for any reason, another physical server running the same virtual machine can take its place. This minimizes any interruption in service.
- Network Virtualization create logical, virtual networks that are decoupled from the underlying network hardware to ensure the network can better integrate with and support increasingly virtual environments.
- Further virtualization types are desktop-, application- and service virtualization

Virtualization of clients is not recommended. Depending on the virtualization software, performance issues (such as, display of multiple video streams or graphic display) may occur.

Desigo CC supports several server virtualization environments and their redundancy options including transparent Network Virtualization. Terminal Server applications, Desktop-, Service- and Application Virtualization are not supported.

The following key components can be virtualized:

- Desigo CC Server
- Video Management Service
- Microsoft SQL Server
- Microsoft IIS Server
- Desigo CC FEP

For a list of the supported virtualization environments (including fault-tolerant options) please refer to

*Part C:* p.46.

**UL/ULC Deployments**
Supported virtualization software in UL/ULC deployments may differ from the ones mentioned before

# 1.3 Cyber Security Concepts - How to Secure the System

## Protection against Casual or Coincidental Violation

Desigo CC complies with the ISA-99/IEC 62443 Security Level: **SL1** .as long as the recommendations described in this document are implemented in full.

## Security Categories

Security in Desigo CC is divided into the following categories:

- **Protection**
  Protection of Desigo CC against unauthorized and malicious use. This includes provision of secure communication that prevents any manipulation of messages as well as validation of users (authentication) to prevent access by unknown users to the system.
- **Authorization**
  Provision of a fine-grained but easy-to-configure authorization model: Provides access to any system resource and functionality in a way that the access rights of users correspond with their capabilities, such as acting as system administrator or personnel manager, and the current operating conditions, such as organization mode and/or the user location.

The features related to *Protection* can be summarized as follows:

- All communication paths between clients and the server provide encryption and protect against replay attacks as well as data manipulation. The communication between the Web Server (IIS) and the Web Clients is always encrypted.
- Communications between the system server and a FEP can be encrypted by Desigo CC.
- Communications between the system server and SQL Server can be encrypted by Desigo CC.
- The runtime data transfer between the system server and IIS can be encrypted by Desigo CC.
- Passwords are handled securely:
  - Encrypted storage and transmission
- Use of public domain algorithms for cryptographic functions, including:
  - AES, DiffieHellmann, RSA, SHA-2, and so on
  - No self-coded algorithms
- Key strengths are defined as general security baselines, for example:
  - Symmetrical encryption uses 256 bit AES or stronger
  - Asymmetrical encryption uses 2048 bit or stronger

The features related to *Authorization* can be summarized as follows:

- The Authorization Model allows controlling access, view, and commanding privileges of users and user groups on a very granular level based on resources/groups. These resources/groups can be workstations, features, applications, system objects, system object properties, and logical groups of any kind for these resources.
- Access to the system is treated intuitively – the UI displays only elements such as menus, buttons, list items, tree nodes, and so on where the user has at least read access.

## 1.3.1 User Management

### User Account Management

**NOTE:**
Desigo CC users can be configured to use local passwords or to use Windows authentication (for example, Active Directory).
Use Windows authentication wherever possible to enhance security, control, and management of passwords.

General security guidelines for Desigo CC user account management (Windows OS):

- Use nominative accounts (do not use generic -group accounts- that are used by multiple persons)
- Rename the default administrator account
- Use strong passwords (e.g.: 12 character including characters with upper case, lower case, special characters, and numbers)
- Change passwords on a regular basis, especially passwords for administrator accounts and the password of the service account (root)
- If accounts are created by default or from a template, use different passwords for each installation
- Do not use the same password for the default administrator account and the service account
- Make sure there is a process in place to disable and then remove (above desired logs' retention time) old/unused user accounts
- Auto-logon features skip the identification of a user and should therefore only be used either in controlled environments, where the effective user can be determined differently, or for users that are only authorized to see non-confidential data

### User Authorization Configuration

User access rights in Desigo CC are determined by four main factors:

- The system must know the user (authentication)
- The user must be assigned a user group
- The user group has the appropriate application rights
- The user group must have the appropriate scope rights

If all of these conditions are met, the user can log on to Desigo CC, and read/write objects and execute tasks, depending on the assigned rights.

For detailed information on how to configure user authorization (users, user groups, application rights, scope rights), see sections *Configuring User Administration* and *Configuring Scopes* in the Desigo CC Online Help.

## 1.3.2 IT Security

| ! | *NOTICE* |
|---|---|
| | The owner of the Desigo CC system is responsible for establishing and maintaining appropriate IT security, in particular by applying virus scanners, deactivating unneeded services and network ports, and by regular patching and updating the operating system and all installed applications. |

## 1.3.3 Communication Security

The communication between Web Clients and the Web Server (IIS) is always encrypted. The runtime data transfer between a FEP and the system server, between the system server and a Web Server, and between the system server and Installed Clients may be encrypted as an option.

The file transfer between the system server and Installed Clients and between the system server and a Web Server is unencrypted for performance reasons.

The communication between the system server and the History Database is unencrypted for performance reasons.

Sensitive data (such as, passwords during authentication or user management configuration) is transferred as encrypted content between the Desigo CC clients and the system server (regardless of the communication encryption).

**NOTE:**
Self-signed certificates are supported to allow local deployments without the overhead of obtaining commercial certificates. When using self-signed certificates, the owner of the Desigo CC system is responsible for maintaining their validity status, and for manually adding them to and removing them from the list of trusted certificates.

Self-signed certificates may only be used in accordance with local IT regulations (some CIO organizations do not allow them, and network scans will identify them). Importing of commercial certificates follows the same procedures.

**NOTE:**
Wireless input devices (especially keyboards) use radio transmission that is often not or inadequately cryptographically protected. Even from greater distances, it is possible to listen in or even plant external data in the system. The use of wireless input devices should be avoided when used in high security environments. If the use of wireless input devices is absolutely necessary, use only devices with proven encryption.
With version 4.0, the Bluetooth (BT) standard includes an encryption mechanism (AES128). In order for it to be effective, all devices must use BT 4.0. Users should also observe the information provided by the manufacturer.

## 1.3.4 License Security

Licensing is important to guarantee the operation of the system within the agreed system limits. Only the system is allowed to change license data.

If a license becomes temporarily unavailable (for example, dongle un-plug) the system continues running fully operational for a demo period of 30 minutes. The system continues to check for the license and shuts down at the end of the demo period, if the license checks are unsuccessful.

Exceeding the limits of the license (for example, by integrating more field system data points than stated in the license), puts the system into Courtesy mode. Phases of Courtesy mode accumulate until a total duration of 30 days is exceeded, then the server shuts down. Unless new licenses are purchased and activated, after a manual restart the system returns into Courtesy-mode strike exceeding and shut down.

Any unauthorized attempt to modify system license data directly in the database (for example, change of the remaining time of a specific license mode) shuts down the system.

## 1.3.5 Stored Data Security

Data is generally stored unencrypted in Desigo CC. Exceptions are sensitive data such as passwords for accessing Desigo CC (hashed), or passwords required by Desigo CC to access field system devices (encrypted).

### Project Data

Runtime data (process image) and engineering data is stored in a file-based database in a subdirectory of the project directory. Data is unencrypted and database access can only be prevented by restricting access to the database files. The project directory must be shared when deploying Installed Clients. It is hence important to restrict access to the **DB** folder in the project directory to the Windows account running the Desigo CC Server.

### Database (HDB)

Historical data is stored in an access-controlled Microsoft SQL Server database. This database should be outside the project folder to allow for independent handling and backup of project data and historical data. It is recommended to encrypt the connection to the History Database when using a remote MS SQL Server.

### Backups of Project or History Database

Backups of the system or archives from the History Database are not encrypted and can get restored on any system. Therefore, it is important to store backups in secure locations and encrypt if necessary (different passwords should be used for different sites).

## 1.3.6 Main Server Folder Shares for Client and FEP Installations

When installing additional Installed Clients, FEPs or a remote Web Server, the project directory needs to be shared and the access rights to the folders must be configured. The local client and the Web Server on the Desigo CC Server do not need file sharing; only access rights to the folders in the project directory need be configured.

ⓘ

NOTE:

**Avoid Exposed Network Shares**
Since exposed network shares could be used to illicitly discover confidential information from the network, restricted use as much as possible. For example, only to the users and the computer that need access.
In Desigo CC, shares are only needed for Installed Clients and the Web Server (unless they are on the same machine), not for the Windows App and Web Clients.
Since these should be reached via dedicated server or control room network, never exposes the shares to the office network or customer intranet (direct or via VPN) and never exposes shares to the Internet.

è See section *Sharing the Project Folder on the Server* in the Desigo CC Online Help.

Please take note the following terms:

- **Windows client account**
  Refers to the user logged on to Microsoft Windows on the client machine; this Windows user can be different from the user logged on to Desigo CC.
- **Web Server account**
  Refers to the account configured in the Desigo CC Web Server installation.

The following subdirectories of the [project] directory are accessed by the client installation (Installed Client or FEP) and the Web Server.

- **Documents**
  Provide read access on all files and subfolders to the Web Server account and all Windows client accounts.
- **Devices, Graphics, Libraries, and Profiles**
  Provide read/write access on all files and subfolders (including the right to delete them, but not the root folder itself) to the Web Server account and all Windows client accounts.
  - **Graphics**
    Access may be restricted to read-only for Windows client accounts that only display but do not configure graphics.
  - **Libraries**
    Access may be restricted to read-only for Windows client accounts that run Desigo CC in Operation mode only.
  - **Profile**
    Provide read access to all Windows client accounts, read/write access to the Web Server account.
- **Shared**
  Provide read access on all files and subfolders to the Web Server account and all Windows client accounts.
- **All other folders**
  Provide read/write access to the [System Account] only ([System Account] is configured in SMC).
  Do not provide access on these folders to any other account!

## 1.3.7 Server Services

The following services are deployed on the Desigo CC Server:

- **GMS_WCCILpmon_[Project Name]**
- **Siemens GMS HDB Service**

- **Siemens GMS Closed Mode Service**
- **Siemens GMS SMC ProjectData Service**
- **SQL Server ([Instance Name])** and **SQL Server Browser**
  Microsoft SQL Server services for the History / MNS Database (if the database is deployed on the Desigo CC Server).
- **WCIILdist.exe** (used in Distributed System Configurations)

Additional services are installed depending on the extension modules deployed (please refer to the respective integration guides), for example:

- **OPC Enum**
  Belongs to the Desigo CC OPC Server
- **UA Local Discovery Server**
  Belongs to the Desigo CC OPC Server
- **UA COM Server Wrapper**
  Belongs to the Desigo CC OPC Server
- **Siemens BT Video API Service**
  This service is part of the Video Extension Module and can also be deployed on a remote machine as an option.
- **VMS Service** (Embedded Siveillance VMS200).
  Installed separately by users, not by the Video Extension Module.

Siemens License Management System deploys additional services. The following services are deployed on FEPs and Installed Clients:

- **GMS_WCCILpmon_[Project Name]**
- **Siemens GMS Closed Mode Service**

# 2 Part B: System Dimensioning Guidelines

This section provides guidelines on how to size Desigo CC system. It is organized as follows: Server, FEP, and Client.

## 2.1 Desigo CC Server

Desigo CC is a memory-based management station.
Each physical or logical entity in the system is represented by a **system object** allocated in memory.

Hardware requirements for Desigo CC Server depend primarily on the number of system objects it shall manage (system size).

The current Desigo CC version supports up to 150,000 system objects per system (project). However, up to 450,000 system objects could be reached with a single server by using a distributed system configuration where several Desigo CC systems are running at the same time (segmented configuration, see 1.2.2.5).

Another, although minor, factor that impacts on Desigo CC Server dimensioning is the number and type of clients.

Finally, the required disk storage space needs to be considered.

Disk storage space is needed for historic data kept in the SQL server and for project data, including attachments and documents.

In order to facilitate hardware configuration choices, reference hardware configurations have been identified and tested:

HW Cat. A: Tailored for All-in-One configurations, up to 25,000 system objects

HW Cat. B: Tailored for medium size Client-Server configurations, up to 50,000

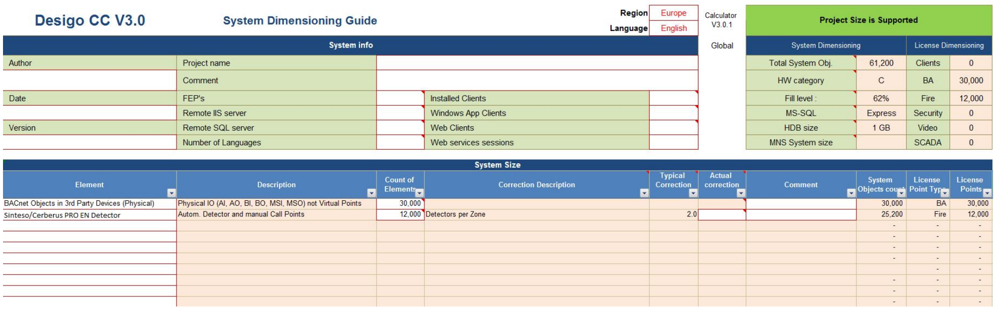
HW Cat. C: Tailored for large Client-Server configurations, up to 100,000 objects

HW Cat. D: Tailored for very large Client-Server configurations, up to 150,000 objects

In case of a system running inside a distributed configuration possible categories are B1, C1 and D1.

è Hardware categories are defined in the *Hardware Category Definitions* section on p.67, both for physical and for virtual environments.

Desigo CC covers a wide variety of solutions so that is impossible, to define simple rules for determining the size. Therefore, a system dimensioning tool is available and estimates system size and disk storage space on the basis of information available at the time of the offer, for example, the number and type of physical points and the expected history data base contents.



Desigo CC V3.0 System Dimensioning Guide

Region Europe
Language English

Calculator V3.0.1

Global

Project Size is Supported

System info

| | | | | |
|---|---|---|---|---|
| Author | Project name | | | |
| | Comment | | | |
| Date | FEP's | | Installed Clients | |
| | Remote IIS server | | Windows App Clients | |
| Version | Remote SQL server | | Web Clients | |
| | Number of Languages | | Web services sessions | |

| System Dimensioning | | License Dimensioning | |
|---|---|---|---|
| Total System Obj. | 61,200 | Clients | 0 |
| HW category | C | BA | 30,000 |
| Fill level : | 62% | Fire | 12,000 |
| MS-SQL | Express | Security | 0 |
| HDB size | 1 GB | Video | 0 |
| MNS System size | | SCADA | 0 |

System Size

| Element | Description | Count of Elements | Correction Description | Typical Correction | Actual correction | Comment | System Objects count | License Point Type | License Points |
|---|---|---|---|---|---|---|---|---|---|
| BACnet Objects in 3rd Party Devices (Physical) | Physical IO (AI, AO, BI, BO, MSI, MSO) not Virtual Points | 30,000 | | | | | 30,000 | BA | 30,000 |
| Sinteso/Cerberus PRO EN Detector | Autom. Detector and manual Call Points | 12,000 | Detectors per Zone | 2.0 | | | 25,200 | Fire | 12,000 |
| | | | | | | | - | - | - |
| | | | | | | | - | - | - |
| | | | | | | | - | - | - |
| | | | | | | | - | - | - |
| | | | | | | | | - | - |
| | | | | | | | - | - | - |
| | | | | | | | - | - | - |
| | | | | | | | - | - | - |

When the required configuration and the number and type of clients have been defined, the system dimensioning tool verifies system feasibility, suggests the appropriate hardware category for the server, the required storage space for the project, the version and the disk space required for the SQL server.

The example in the previous picture refers to a system with 30,000 BACnet points and 12,000 Fire detectors, with sufficient storage for 3 years of trends and activity logs online.

è To obtain the latest version of the System Dimensioning Guide Calculator, please refer to Siemens Intranet: https://intranet.for.siemens.com/cms/041/en/business/products/Pages/desigocc.aspx

è or Siemens Extranet: http://www.siemens.com/bt/partner-extranet (Click the “Download” button on the start page and then select “Tools and software”).

## 2.2 Distributed Systems

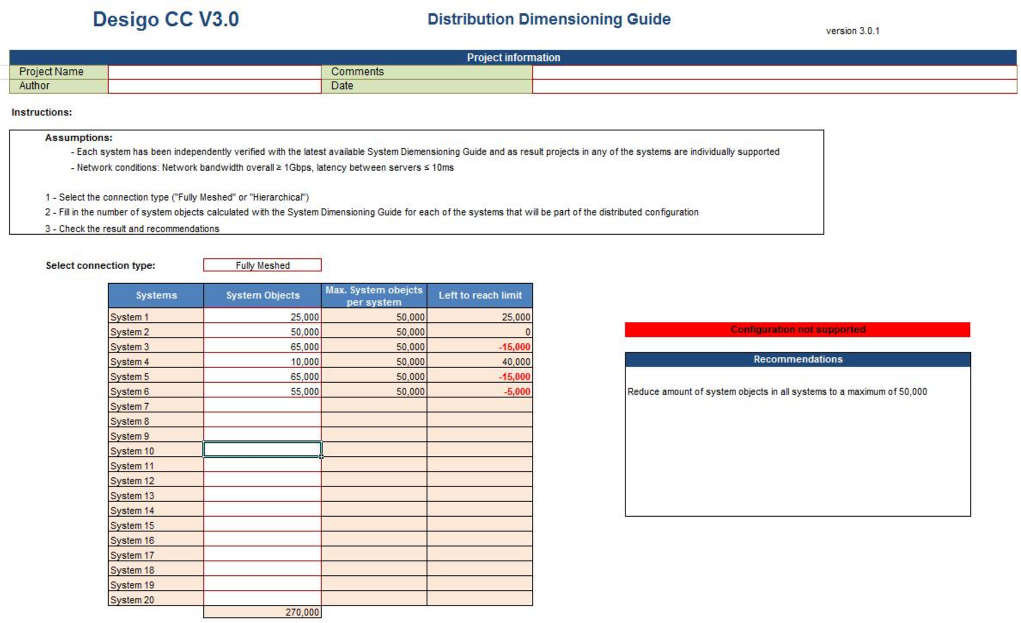
A dimensioning tool is available to verify the feasibility of distributed configurations.

Systems that will be part of a distributed configuration must be dimensioned individually first before using the Distribution dimensioning tool.

The input of the tool is the desired topology, fully meshed or hierarchical, and the number of system objects for each of the projects  that will be part of the distributed configuration.

As a result the tool provides a clear indication of the support for such a configuration and in case of non-support, some possible recommendations to change the situation so that the configuration becomes supported.

The tool is purely based on the results from system tests and will be refined progressively with the feedback of new system tests and field experience.



Desigo CC V3.0

Distribution Dimensioning Guide

version 3.0.1

Project information

|  |  |  |  |
|---|---|---|---|
| Project Name |  | Comments |  |
| Author |  | Date |  |

Instructions:

Assumptions:

- Each system has been independently verified with the latest available System Diemensioning Guide and as result projects in any of the systems are individually supported
- Network conditions: Network bandwidth overall ≥ 1Gbps, latency between servers ≤ 10ms

1 - Select the connection type ("Fully Meshed" or "Hierarchical")

2 - Fill in the number of system objects calculated with the System Dimensioning Guide for each of the systems that will be part of the distributed configuration

3 - Check the result and recommendations

Select connection type: Fully Meshed

| Systems | System Objects | Max. System obejcts per system | Left to reach limit |
|---|---|---|---|
| System 1 | 25,000 | 50,000 | 25,000 |
| System 2 | 50,000 | 50,000 | 0 |
| System 3 | 65,000 | 50,000 | -15,000 |
| System 4 | 10,000 | 50,000 | 40,000 |
| System 5 | 65,000 | 50,000 | -15,000 |
| System 6 | 55,000 | 50,000 | -5,000 |
| System 7 |  |  |  |
| System 8 |  |  |  |
| System 9 |  |  |  |
| System 10 |  |  |  |
| System 11 |  |  |  |
| System 12 |  |  |  |
| System 13 |  |  |  |
| System 14 |  |  |  |
| System 15 |  |  |  |
| System 16 |  |  |  |
| System 17 |  |  |  |
| System 18 |  |  |  |
| System 19 |  |  |  |
| System 20 |  |  |  |
|  | 270,000 |  |  |

Configuration not supported

Recommendations

Reduce amount of system objects in all systems to a maximum of 50,000

Dedicated Microsoft SQL Server

If the HDB/MNS is deployed on a SQL server running on a server other than the Desigo CC Server, the recommended hardware and software configuration is described below.

| Microsoft SQL Server |  |
|---|---|
| Description | A dedicated server for the SQL Database Server |
| Recommended hardware category | **C** (XEON variant) |
| Recommended software environment | Windows Server 2012 R2, or 2016 multilingual, 64 bit<br>Microsoft SQL Server Server 2012, SQL Server 2014 or SQL Server 2016 (Standard or Enterprise) |

## 2.3 FEPs

If system configuration requires distribution of field network connectivity, the recommended hardware and software configuration for FEP is described below.

| Front End Processor (FEP) |  |
|---|---|
| Description | Enhancement of connectivity capacity with distributed field network drivers |
| Recommended hardware category | Size of system connected to FEP <= 25,000 objects: **A**<br>Size of system connected to FEP > 25,000 objects: **B** |
| Supported software environment | Windows 7 Professional, Service Pack 1, 64 bit<br>Windows 10 Professional and Enterprise, 64 bit |
| Network requirements | Local network<br>Single subnet<br>100 Mbps up/down<br>Latency less than 10 ms<br>For the integration of XNET Fire Safety Systems, the server hardware must have a PCI slot for the NCC-2F card |
| Recommendation | Max 40 drivers per FEP. Total per system: 100 (see 3.1.1)<br>Max 5 FEP |

# 2.4 Clients

## 2.4.1 Installed Clients

| Installed Client | |
|---|---|
| Description | Statically installed, highest performance in local network. |
| Recommended hardware category | A (Note: 256 GB SSD hard disk is enough for clients) |
| Supported software environment | Windows 7 Professional, Service Pack 1, 64 bit<br>Windows 10 Professional and Enterprise, 64 bit<br>Windows Server 2012 R2 and Windows Server 2016 |
| Network requirements | Local network:<br>Preferred for: Control Rooms and regular engineering and commissioning, including data import.<br>Mostly single subnet<br>100 Mbps up/down<br>Latency less than 10 ms |
| | Corporate networks across site to site connectivity:<br>Different subnets (often secured with firewalls/DMZ):<br>Minimum 10 Mbps up/down |
| | Remote connection through VPN :<br>Recommended only for casual remote operation and casual remote engineering (no data import)<br>Multiple subnets<br>Minimum 10 Mbps up/down<br>Latency less than 100 ms |

## 2.4.2 Windows App Clients

| Windows App Client | |
|---|---|
| Description | Client software can be statically or temporarily downloaded via Desigo CC Web Server. |
| Recommended hardware category | A (Note: 256 GB SSD hard disk is enough for clients) |
| Supported software environment | Windows 7 Professional, Service Pack 1, 64 bit<br>Windows 10 Professional and Enterprise, 64 bit<br>Windows Server 2012 R2 and Wisndows Server 2016 |
| Network requirements | Local network<br>Multiple subnets<br>100 Mbps up/down<br>Latency less than 10 ms |
| | Corporate networks across sites, using SHDSL site-to-site connectivity:<br>Different subnets (often secured with firewalls/DMZ):<br>Minimum 2 Mbps up/down |
| | Remote connection through VPN, using ADSL<br>Recommended for casual remote operation and casual remote engineering (no data import)<br>Multiple subnets<br>Minimum 512 Kbps up/6 Mbps down<br>Latency less than 100 ms |

## 2.4.3 Web Clients

| Web Clients | |
|---|---|
| Description | Client running in a browser shell |
| Recommended hardware category | A (Note: 256 GB SSD hard disk is enough for clients) |
| Supported software environment | Windows 7 Professional, Service Pack 1, 64 bit<br>Windows 10 Professional and Enterprise<br>Windows 2012 R2 and 2016<br>Microsoft Internet Explorer 11 |
| Network requirements | Local network<br>Multiple subnets<br>100 Mbps up/down<br>Latency less than 10 ms |
| | Corporate networks across sites, using SHDSL site-to-site connectivity:<br>Different subnets (often secured with firewalls/DMZ):<br>Minimum 2 Mbps up/down |
| | Remote connection through VPN, using ADSL<br>Wide area network<br>Multiple subnets<br>Minimum 512 kbps up/6 Mbps down (ADSL)<br>Latency less than 100 ms |

## 2.4.4 Monitors

### Monitor Resolution

For graphical user interface operation on Installed, Windows App, or Web Clients, a minimum resolution of 1600 x 900 pixels is required, but full HD (1920x1080) is recommended.

### Multiple-Monitor Management

Desigo CC Installed or Windows App Client can take advantage of multiple monitors, when available and any system window such as, System Manager, Investigative Treatment, or Help can be moved from the default monitor to a second monitor. The Summary bar remains on the primary monitor (cannot be moved).

NOTE:

The current system window settings in the multiple monitors are not retained when closing the client session, see the *User Guide.*

# 3 Part C: System Limits, Restrictions and Compatibility

## 3.1 Desigo CC System Limits and Restrictions

### 3.1.1 Non-distributed systems

Please ensure that the project in the Management System Server does not reach any of the system restrictions listed in the following table.

| Desigo CC | |
|---|---|
| Topic | System Limits |
| Maximum number of objects handled by the Management System Server | 150,000 (requires HW Category D, restricted to 2 languages) |
| Maximum number of Installed Clients | 10 |
| Maximum number of Windows App and Web Clients | 27 |
| Maximum number of active Web service sessions | 10 (if IIS runs on Windows 7/10)<br>100 (if IIS runs on Windows Server 2012 R2/2016) |
| Maximum number of FEPs | 5 |
| Maximum number of drivers per FEP | 40 |
| Maximum number of drivers per Server. See note below | Local: 20 (in a Server)<br>Total: 100 (split between the local Server and a minimum of 2 FEPs) |
| Maximum of tags exposed by the OPC Server | 40,000 |
| Maximum number of integrated OPC Servers per OPC Client driver | 20 |
| Maximum name length of OPC tags integrated via OPC Client driver | 100 |
| Max. number of SORIS objects per SORIS driver | 10,000 |

| Desigo CC | |
|---|---|
| Topic | System Limits |
| Minimum network throughput for Windows App or Web Clients using VPN | Minimum 512 kbps up/6 Mbps down (ADSL)<br>Maximum Latency: 100 ms |
| Alarm load<br>(rate of new alarms) | Desigo CC has been tested for the alarm loads defined below. Do not exceed:<br>Constant load of 1 alarm per second in average<br>10 alarms per second in average over a time period of 20 minutes<br>50 alarms per second over a time period of 20 seconds (alarm burst)<br>(The test was measured with one alarm burst per hour).<br>"Alarm per second” indicates the arrival of a new event/fault/alarm and includes the handling cycle until it is closed later. If Operating Procedures (OPS) are used during event handling, the maximum load is reduced depending on the complexity of the OPS. |
| Maximum number of Activity logs per day | 1,000,000 |
| Maximum number of Event records per day | 1,000,000 |
| Maximum number of Trend records per day | 4,200,000 |
| Maximum number of reactions defined | 800 |
| Maximum number of reactions that can be executed simultaneously | 320 |

**NOTE:**

Each driver adds approximately 25 seconds to the overall startup time on a system installed in a Class D hardware category. For hardware categories refer to page 67.

### 3.1.1 Distributed system configurations

Given all the variants that could exist in distributed system configurations, it is impossible to test and give precise limits for all the possible scenarios. Tests have been performed for some given scenarios and results are presented here as a guideline for configurations closed to these examples.  For queries on support of any other configuration, use the Distribution Dimensioning Guideline or contact Customer Support.

Maximum number of systems, remote installed clients (including FEPs) and simultaneous Windows app / web clients have been proved to work for three different quantities of system objects. For any other limit, please refer to the previous section.

| Fully meshed | | |
|---|---|---|
| 25,000 objects per system | Maximum number of systems | 10 |
| | Maximum number of remote installed clients per system | 2 |
| | Maximum number of Windows app and web clients per system | 10 |
| 50,000 objects per system | Maximum number of systems | 6 |
| | Maximum number of remote installed clients per system | 2 |
| | Maximum number of windows app and web clients per system | 10 |
| 100,000 objects per system | Maximum number of systems | 4 |
| | Maximum number of remote installed clients per system | 2 |
| | Maximum number of windows app and web clients per system | 10 |
| 150,000 objects per system | Maximum number of systems | 3 |
| | Maximum number of remote installed clients per system | 2 |
| | Maximum number of windows app and web clients per system | 10 |

Number of systems in following table refer to the supervised systems

| Hierarchical | | |
|---|---|---|
| 25,000 objects per system | Maximum number of systems | 20 |
| | Maximum number of remote installed clients per system | 2 |
| | Maximum number of Windows app and web clients at hierarchical supervisor | 10 |
| | Maximum number of Windows app and web clients at a supervised system | 27 |
| 50,000 objects per system | Maximum number of systems | 12 |
| | Maximum number of remote installed clients per system | 2 |
| | Maximum number of Windows app and web clients at hierarchical supervisor | 10 |
| | Maximum number of Windows app and web clients at a supervised system | 27 |
| 100,000 objects per system | Maximum number of systems | 6 |

| Hierarchical | | |
|---|---|---|
| | Maximum number of remote installed clients per system | 2 |
| | Maximum number of Windows app and web clients at hierarchical supervisor | 10 |
| | Maximum number of Windows app and web clients at a supervised system | 27 |
| 150,000 objects per system | Maximum number of systems | 5 |
| | Maximum number of remote installed clients per system | 2 |
| | Maximum number of Windows app and web clients at hierarchical supervisor | 10 |
| | Maximum number of Windows app and web clients at a supervised system | 27 |

| Network requirements for distribution | |
|---|---|
| Network bandwidth | ≥1Gbps |
| Network latency between servers | ≤10ms |

In a hierarchical configuration, the supervisor server should not contain any kind of integration (either local, or via FEP). This statement becomes more important the bigger the amount of system objects in the supervisor is. The limits indicated in the table above have been tested with no subsystems or FEPs connected to the supervisor.

If number of servers in a distributed system configuration is bigger than 5, consider, the use of SQL Server Standard edition is recommended.

Class **D1** Hardware category should be used for the supervising server of a hierarchical configuration.

è Hardware categories are defined in the *Hardware Category Definitions* section on p.67, both for physical and for virtual environments.

NOTE:

Hybrid topologies have not been considered in the System Description and have not been tested. However, feasibility and design of such topologies can be consulted through Customer Support.

## 3.2 System Limits and Restrictions of Mass Notification

The following system limits specific to the Mass Notification extension module of Desigo CC Version 3.0 should be considered.

| Scope | System limits[10] | Comment |
|---|---|---|
| Recipient Users | 20,000 | Engineered recipient users with recipient user devices of any kind. |
| Templates | 200 | Engineered incident and notification templates |
| System Devices | 2,500 | Engineered devices |

The table below shows limits for device types specific to Mass Notification as well as additional limits to meet certain timing requirements, if required.

| Device | Maximum Size | Size to Meet Timing Require-ments | Timing Requirement for Single-Device Deployment | Comment |
|---|---|---|---|---|
| Single Zone Audio - Message | 150 devices | 150 devices | <(8s + relay activation time) to play message | |
| Single Zone Audio - Live Announcement | 150 devices | 150 devices | Until operator phone rings: <3s<br>From phone pick up to talk: <(7s + relay activation delay defined in device settings) | |
| Single Zone Audio - Blue Light | 150 devices | 150 devices | <(8s + DTMF activation sequence) to play message | |
| Multi Zone Audio – Message | 150 devices | 150 devices | <(8s + relay activation time) to play message | |
| Multi Zone Audio – Live Announcement | 150 devices | 150 devices | Until operator phone rings: <3s<br>From phone pick up to talk: <(7s + relay activation delay defined in device settings) | |
| Media display (with preloading) | 300 devices | 300 devices | <10s until preloaded content is displayed | Time to start playing content after incident initiation will increase if media content is not preloaded, and if TV „remote control“ commands are configured to make sure that display reacts to commands such as powering on as well as setting the volume and channel. |
| Adaptive | 300 devices | 300 devices | <10s to end of delivery to sign | |

| Device | Maximum Size | Size to Meet Timing Require-ments | Timing Requirement for Single-Device Deployment | Comment |
|---|---|---|---|---|
| AND Display | 300 devices | 300 devices | <10s to end of delivery to sign | |
| SMTP email | 1,000 recipient users | 250 recipient users | Start of delivery to SMTP server: <10s<br>End of delivery to SMTP server: <60s | This is the Desigo Mass Notification internal limit for SMTP. Any limitations of the customer's SMTP server are not considered. |
| Bulk Notification (email) | 20,000 recipient users | 4,000 recipient users | Start of delivery to provider: <10s<br>End of delivery to provider: <60s | Delivery time to end device is beyond control of Desigo Mass Notification and depends on the provider. |
| Desktop Notification (hosted on separate server) | 20,000 recipient users | 4,000 recipient users | Start of delivery to desktop server: <10s<br>End of delivery to desktop server: <60s | Recommended to use two separate physical servers (one server for the Desigo CC with Mass Notification software and one server for the Desktop Notification server software) to obtain the best system performance and better system security. Dedicated physical server required if more than 1000 desktop notification clients are targeted. |
| Facebook | 3 accounts | 3 accounts | <10s to end of delivery to account | |
| Twitter | 3 accounts | 3 accounts | <10s to end of delivery to account | |
| Web Feed Publisher | 3 feeds | 3 feeds | <10s to end of delivery to account | |
| ASCII Input | 100 devices | 100 devices | <10s to raise event | |
| Digital Input | 100 devices | 100 devices | <10s to raise event | |
| ESPA 4.4.4 Interface | 50 recipient users | 50 recipient users | Start of delivery to gateway: <10s<br>End of delivery to gateway: <60s | |
| GSM Gateway | 15 recipient users | 15 recipient users | Start of delivery to gateway: <10s<br>End of delivery to gateway: <60s | |
| SMPP SMS Gateway | 2,000 recipient users | 2,000 recipient users | Start of delivery to provider: <10s<br>End of delivery to provider: <60s | |
| Relay Output | 200 devices | 200 devices | <10s to end of delivery to device | |

| Device | Maximum Size | Size to Meet Timing Require-ments | Timing Requirement for Single-Device Deployment | Comment |
|---|---|---|---|---|
| Web feed input | 5 feeds | 5 feeds | <= configured polling interval to raise event | |
| Hotline | 48 extensions | 48 extensions | <10s to end of delivery to h.line | |

Deployment sizes to meet timing requirements have been verified for single device type and single discipline deployments only. Timing performance cannot be guaranteed when exceeding those limits and/or deploying multiple Mass Notification device types.

[10] *The figures provided in the table reflect numbers evaluated during system scalability testing.*

## 3.2.1 System Size of Mass Notification

Determine the Mass Notification system size based on the required number of devices to be integrated with Mass Notification. For example, if a Mass Notification system integrates with 50 Adaptive displays (*Small* size) and 120 single audio zone devices (*Large* size), then the resulting overall Mass Notification system size is the larger of the two, in this case *Large*.

| Service Class | Device Type | Small | Medium | Large |
|---|---|---|---|---|
| Max. number of running Mass Notification drivers on main Desigo CC server (use FEP for more drivers) | | 5 | 5 | 5 |
| Sign support | Adaptive displays | 100 | 200 | 300 |
| Sign support | Prolite displays | 100 | 200 | 300 |
| Media display support | Media display devices | 100 | 200 | 300 |
| Audio zone support | Multi Zone Audio device | 20 | 60 | 150 |
| Audio zone support | Single Zone Audio device | 20 | 60 | 150 |
| PBX Extended (shared with Dial-In) | Hot Line device | 10 | 30 | 48 |
| Desktop messaging support | Desktop Notification device | 5,000 | 10,000 | 20,000 |
| Hosted messaging support | Bulk Notification Email | 5,000 | 10,000 | 20,000 |
| Hosted messaging support | Bulk Notification SMS | 5,000 | 10,000 | 20,000 |
| Hosted messaging support | Bulk Notification phone calls | 5,000 | 10,000 | 20,000 |
| Local network messaging support | SMTP Email device | 250 | 500 | 1,000 |
| Facebook support | Facebook device | 3 | 3 | 3 |
| Twitter support | Twitter device | 3 | 3 | 3 |
| RSS support | Web Feed Publisher device | 3 | 3 | 3 |
| Input monitoring | ASCII Input device | 25 | 50 | 100 |
| Input monitoring | Digital Input device | 25 | 50 | 100 |
| RSS support | Web Feed Input device | 5 | 5 | 5 |
| Relay support | Relay Output device | 50 | 100 | 200 |
| Cellular modem support | GSM Gateway device | 50 | 50 | 50 |

### Hardware Sizing

Determine the required server size from the following tables, based on the Mass Notification system size that you determined in the section above. Please note that multi-discipline deployments will require larger server sizes to accommodate the load caused by concurrently running extension modules. HW Classes A,B,C,D are described below in Chapter 3.7.

### Desigo CC with Mass Notification only

| Mass Notification Size | Small | Medium | Large |
|---|---|---|---|
| Server Hardware Class | Class A | Class B | Class C |

### Desigo CC with multi-discipline configuration (Mass Notification plus additional extension modules)

Due to the specific resource and performance requirements of the Mass Notification extension module, the Server Hardware Class as determined according to the underlying Desigo CC System Description may need to be corrected upwards, depending on the Mass Notification system size. Use the following Mass Notification - specific table to choose the correct server hardware class and CPU requirements.

For Desigo CC projects with MNS, the number of logical cores is also important, for its performance. 1 physical CPU core corresponds to 2 logical CPU cores. In addition to the standard HW categories A,B,C,D mentioned above, the following 3 categories have to be considered.

- B1 = Class B, CPU with at least 6 logical cores
- C1 = Class C, CPU with at least 2x6 logical cores
- D1 = Class D, CPU with at least 2x8 logical cores

| Object / Mass Notification Size | 0..25,000 | 25,001 .. 50,000 | 50,001 .. 100,000 | 100,001 .. 150,000 |
|---|---|---|---|---|
| Small | Class A | Class B | Class C | Class D |
| Medium | B1 | B1 | D1 | D1 |
| Large | C1 | D1 | D1 | D1 |

## 3.3 Communication Ports and Protocols

The tables in the following sections list the ports provided and used by the Desigo CC components on the different configurations. The ports that are used depend on the actual deployment and subsystem integration of the system as a whole. Only ports that are used beyond machine boundaries and hence important for firewall and router configurations are marked in the tables columns on the right.

**NOTE:**
To support initial port configurations on customer sites, the System Management Console (SMC) displays all ports used for communication between the various Desigo CC components.
Communication ports that are not needed in the actual deployment must be locked down in the firewall for the corresponding host.

## 3.3.1 Ports Used for Client-Server and Server-Server Communication

If a firewall is placed between clients and the server or between server nodes, the ports on the hosting machine must be opened to allow communication. If the firewall also restricts outbound communication, the corresponding exceptions must be added to the firewall rules.

Which ports are required for cross-machine communication depends partly on the security configuration of the system server. The system server can be configured as stand-alone, secure, or non-secure in SMC.

In a *stand-alone configuration*, all ports for the SIMATIC Platform are bound to local host communications, that is, the ports are not accessible from other machines. The Proxy Manager which provides the entry point for the secure communication is not get started.

In a *secure configuration*, the SIMATIC Platform communication ports are bound to local host communication, with the exception of the port for the Proxy Manager. The Proxy Manager provides the entry point for the secure communication on the server (to clients having matching SSL certificates deployed). Unencrypted SIMATIC Platform communication across machine boundaries is disabled.

In a *non-secure configuration*, all ports for the SIMATIC Platform communication are externally accessible. The SIMATIC Platform communications are not encrypted. The Proxy Manager is not started.

## Port Usage Across Machine Boundaries for Client-Server and Server-Server Communication

| Core services on Main Server | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Providing Component | | | | | Remote Consumer (connects to this port) | | | | | | | |
| Component, Executable | Default Port | Port Configuration | Protocol - Comment | Port Exposure to Other Machines in the Network | Installed Client (Secure) | Installed Client (Non-secure) | Windows App Client | Web Client | FEP (Secure) | FEP (Non-secure) | Separate Web Server | Remote system (Secure) |
| Data Manager WCCILdata.exe 1) | TCP: 4897 UDP: 4897 | SMC | SIMATIC Platform (WinCC OA) Communication | Exposed if project is set to Non-secure in SMC | | X6) | | | | X8) | | |
| Event Manager WCCILevent.exe 1) | TCP: 4998 UDP: 4998 | SMC | SIMATIC Platform (WinCC OA) Communication | Exposed if project is set to Non-secure in SMC | | X6) | | | | X8) | | |
| Distribution Manager WCIILdist.exe | TCP: 4777 UDP: 4777 | SMC | Simatic Platfrom (WinCC OA) Communication | Exposed only if project is configured for distribution.in non secure mode in SMC | | | | | | | | |
| HDB Reader WCCOAHDBReader.exe 2) | TCP: 7774 UDP: 7774 | SMC | SIMATIC Platform (WinCC OA) Communication | Exposed if project is set to Non-secure in SMC | | X7) | | | | X7) | | |
| SSL Proxy Manager WCCILproxy.exe 1) | TCP: 5678 UDP: 5678 | SMC | SIMATIC Platform (WinCC OA) Communication (SSL encrypted) | Exposed if project is set to Secure in SMC | X7) | | | | X7) | | | X 11) |
| CCom Manager WCCOACComMgr.exe 2) | TCP: 8000 | SMC | HTTP(S) - WCF Web Service | Always exposed | | | | | | | X9) | |
| SMC Service Siemens.Gms.Smc.WCFWindows ServiceHost.exe 2) | TCP: 8888 | SMC | HTTP - WCF Service | Always exposed | X5) | X5) | | | X5) | X5) | | |

| Core services on Main Server | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Providing Component | | | | | Remote Consumer (connects to this port) | | | | | | | |
| Component, Executable | Default Port | Port Configuration | Protocol - Comment | Port Exposure to Other Machines in the Network | Installed Client (Secure) | Installed Client (Non-secure) | Windows App Client | Web Client | FEP (Secure) | FEP (Non-secure) | Separate Web Server | Remote system (Secure) |
| Project Monitoring Service GMS_WCCILpmon_[ProjectName].exe [1)] | TCP: 4999 | SMC | http/pmon protocol<br>Only used for communication of components on the local machine | Never exposed | | | | | | | | |
| Microsoft IIS | TCP: 80 | SMC | HTTP | Always exposed | | | X | X | | | | |
| Microsoft IIS | TCP: 443 | SMC | HTTPS | Always exposed | | | X | X | | | | |
| Microsoft SQL Server Browser sqlbrowser.exe | UDP: 1434 | SQL Server | | Depends on SQL Server configuration<br>Default: exposed | | | | | | | | |
| Microsoft SQL Server DB instance (HDB) sqlserver.exe | TCP: variable [3)] | SQL Server | | Depends on SQL Server configuration<br>Default: exposed | | | | | | | | |
| File and Printer Sharing (NetBIOS Session Service connections) | TCP: 139 | n/a | TCP | | X | X | | | X | X | X | |
| File and Printer Sharing (Server Message Block transmission and reception via Named Pipes) | TCP: 445 | n/a | TCP | | X | X | | | X | X | X | |
| X: port needs to get configured in the firewall of the main server for inbound communication, if the host is protected by a firewall | | | | | | | | | | | | |

| Deployment variants: remote IIS and remote SQL Server | | | | | | | |
|---|---|---|---|---|---|---|---|
| Component, Executable | Default Port | Port Configuration | Protocol - Comment | Port exposure | Windows App Client | Web Client | Main Server |
| Microsoft IIS on separate Web Server | TCP: 80 | SMC or IIS | HTTP | | X | X | |
| Microsoft IIS on separate Web Server | TCP: 443 | SMC or IIS | HTTPS | | X | X | |
| Microsoft SQL Server Browser<br>sqlbrowser.exe | UDP: 1434 | SQL Server | | | | | X [10] |
| Microsoft SQL Server DB instance (HDB)<br>sqlserver.exe | TCP: variable [3] | SQL Server | | | | | X [10] |

| Core services on FEP | | | | |
|---|---|---|---|---|
| Component, Executable | Default Port | Port Configuration | Protocol - Comment | Port exposure |
| PMON service<br>GMS_WCCILpmon_[ProjectName].exe [1] | TCP: 4999 | SMC | HTTP/PMON protocol<br>Only used for communication of components on the local machine | Never exposed |

| Optional services on Main Server | | | | | | |
|---|---|---|---|---|---|---|
| Component, Executable | Default Port | Port Configuration | Protocol - Comment | Port exposure | Separate Web Server | 3rd Party OPC Client outside Main Server |
| Web Service Interface<br>WCCOAWsi.exe [2)] | TCP: 8080 | SMC | HTTP(S) - REST Web Service | Always exposed | X | |
| OPC DA<br>Siemens.Gms.OPCServer.exe | TCP: 135<br>UDP: 135 | | RPC End Point Mapping | | | X |
| OPC UA: Local Discovery Server<br>Siemens.Gms.OPCServer.exe | TCP: 4840 | | OPC/TCP | | | X |
| OPC UA: Local Discovery Server<br>Siemens.Gms.OPCServer.exe | TCP: 4883 | | HTTPS | | | X |
| OPC UA: Local Discovery Server<br>Siemens.Gms.OPCServer.exe | TCP: 52601 | | HTTP | | | X |
| OPC UA: UA Wrapper<br>Siemens.Gms.OPCServer.exe | TCP: 48400 | | OPC/TCP | | | X |
| OPC UA: UA Wrapper<br>Siemens.Gms.OPCServer.exe | TCP: 48401 | | HTTP | | | X |

## NOTES:

**Directories of the Host Process**

1) Located in:
- C:\Siemens\WinCC_OA\3.15\bin\

2) Located in:
- [Installation Directory]\GMSMainProject\bin\

**Variable Ports**

3) The port of a Microsoft SQL Server named instance is by default variable.
See the Microsoft SQL Server documentation on how to configure a fixed port for a named instance.

**Consumer**

5) SMC

6) Executables on the client installation.
- [Installation Directory]\GMSMainProject\bin\Siemens.Gms.ApplicationFramework.exe
- C:\Siemens\WinCC_OA\3.15\bin\WCCOActrl.exe

7) Executables on the client installation.
- [Installation Directory]\GMSMainProject\bin\Siemens.Gms.ApplicationFramework.exe

8) Executables on the FEP installation, opening outbound connections.
- C:\Siemens\WinCC_OA\3.15\bin\WCCOActrl.exe
Additional executables on the FEP depend on the driver type.
- BACnet: [Installation Directory]\GMSMainProject\bin\WCCOAGmsBACnet.exe
- SNMP: C:\Siemens\WinCC_OA\3.15\bin\WCCOAsnmp.exe

9) Microsoft IIS

10) - [Installation Directory]\GMSMainProject\bin\WCCOAHDBReader.exe
- [Installation Directory]\GMSMainProject\bin\WCCOAHDBWriter.exe
- [Installation Directory]\GMSMainProject\bin\WCCOAReportMan.exe

11) - [Installation Directory]\GMSMainProject\bin\WCCOACoHoMngr.exe

## 3.3.2 Ports Used for Field System Communications

| Field System | Hosts | Component/Process | Default Ports | Port Configuration | Comment | Protocol |
|---|---|---|---|---|---|---|
| APOGEE P2 | Main Server, FEP | APOGEE P2 driver WCCOAApogeeDrv.exe [2] | TCP: 3001<br>UDP: 3001 | APOGEE Network SnapIn | Required for APOGEE Ethernet Microserver (AEM) | |
| APOGEE P2 | Main Server, FEP | APOGEE P2 Driver WCCOAApogeeDrv.exe [2] | TCP: 5033<br>UDP: 5033 | APOGEE Network SnapIn | Required for APOGEE Ethernet networks | |
| APOGEE P2 | Main Server, FEP | APOGEE P2 Driver WCCOAApogeeDrv.exe [2] | TCP: 5441<br>UDP: 5441 | no | Required for APOGEE Ethernet networks (diagnostic channel) | |
| BACnet | Main Server, FEP | BACnet Driver WCCOAGmsBACnet.exe [2] | UDP: 47808 [3] | BACnet SnapIn | Communication with BACnet field systems (APOGEE BACnet, Desigo PX, Desigo TRA, FS20) | BACnet/IP |
| Modbus | Main Server, FEP | Modbus Driver WCCOAmod.exe [1] | TCP: 502 | Modbus SnapIn | Communication with Modbus TCP devices | Modbus/TCP |
| OPC | Main Server | OPC Driver WCCOAopc.exe [1] | TCP: 135<br>UDP: 135 | no | | OPC/TCP |
| OPC | Main Server | OPC Driver WCCOAopc.exe [1] | TCP: variable [5] | Windows Registry | | OPC/TCP |
| SIMATIC S7 | Main Server, FEP | SIMATIC S7 Driver WCCOAs7.exe [1] | TCP: 102 | no | Communication with S7 PLC (also for SICLIMAT X) | SIMATIC S7 Protocol |
| SNMP | Main Server, FEP | SNMP Driver WCCOAsnmp.exe[1] | UPD: 161[4] | SNMP Network Configuration SnapIn | | SNMP/IP |
| SPC | Main Server, FEP | SPC Driver WCCOASPC.exe [2] | TCP: 50000<br>UDP: 50000 | SPC Driver SnapIn | EDP Receiver Id Port | |
| XNET | Main Server, FEP | XNET Driver NCCGMS.exe [2] | TCP: 1977 | XNET Driver SnapIn | | |

NOTES:

1) File located in:
 - C:\Siemens\WinCC_OA\3.13\bin\

2) File located in:
 - [*Installation Directory*]\GMSMainProject\bin\

3) Default port for the first BACnet driver is UDP: 47808.
The port can get changed; each additional driver needs another UDP port.

4) Default port for the first SNMP network is UDP: 161.
The port can be changed; any additional network needs another UDP port.

5) Four ports for OPC Client-Server communication. Default variable range from 1024 through 5000 (settable using registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet)

The integration of additional Extension Modules in Desigo CC (for example, Video Extension Module) can require additional ports. See the documentation on the corresponding Extension Modules for further information.

Deployment variants of the Siemens License Management may also require additional ports. See the documentation on the License Management Utility for further information.

NOTE:
**Separate Field Automation Networks!**
Generally separate field automation networks and not connected to the office network. Some devices offer web interfaces for configuration or extended status information. If these are intended to be displayed on the office network or inside a Desigo CC client, set up selective routing between the automation network and the office network (only ports and sub networks from known communication relations).

### 3.3.3 Ports Used for Remote Notification Systems

| Outbound connections used by the Host to connect to remote notification systems | | | | | |
|---|---|---|---|---|---|
| Hosts | Component/Process | Port | Port Configuration | Comment | Protocol |
| Main Server | ESPA driver<br>WCCOAGmsCoHoMngr.exe 2) | variable | RENO SnapIn (Pager) | Communication with ESPA Pager modem | ESPA 4.4.4 |
| Main Server | GSM driver<br>WCCOActrl.exe 1) | variable | RENO SnapIn (SMS) | Communication with GSM modem | GSM |
| Main Server | Mail<br>WCCOActrl.exe 1) | TCP: 25, 110, 143 | RENO SnapIn (Mail) | Communication with mail servers. It can be unsecure or secured with SSL or TLS protocols. | SMTP, POP3, IMAP (se-cured with SSL or TLS) |
| Main Server | TAP driver<br>Siemens.Gms.RENO.TAPDevMgr.exe 2) | variable | RENO SnapIn (Pager) | Communication with TAP Pager modem | TAP |

NOTES:

1) File located in:
 - C:\Siemens\WinCC_OA\3.15\bin\

2) File located in:
 - [*Installation Directory*]\GMSMainProject\bin\

## 3.4 IT Environment Compatibility

This section identifies Desigo CC software compatibility with external software relating to its operation.

### 3.4.1 Operating Systems

The Desigo CC Server, FEP, and Installed Clients run on the following Microsoft operating systems and editions:

- Microsoft® Windows 7 64-bit (Professional and Enterprise)
- Microsoft® Windows 10 64-bit (Professional and Enterprise)
- Microsoft® Windows Server 2012 R2 64-bit
- Microsoft® Windows Server 2016 64-bit

Desigo CC is compatible with .NET Framework version 4.6.2 or higher.

Web Clients and Windows App Clients run on following Microsoft operating systems and editions:

- Microsoft® Windows 7 64-bit (Professional and Enterprise)
- Microsoft® Windows 10 64-bit (Professional and Enterprise)

Run Web Clients with Microsoft Internet Explorer 11.

NOTE:
**UL/ULC for Fire applications**
Microsoft Server 2016 64-bit is not approved yet for Fire applications

NOTE:
**Not Supported Microsoft Windows OS:**

- 32-bit operating systems
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012

**Local Language Operating System Support**
Desigo CC Server and Microsoft SQL Server are supported and tested using the English edition of the recommended Microsoft operating systems. For support of *Multilingual User Interface* (MUI) packages, Windows Ultimate or Windows Server edition operating systems must be installed.
For use of native versions of Windows, please contact the local distributor for compatibility of specific versions (for example: the native German or French professional editions).

## 3.4.2 Virtualization

Desigo CC is compatible with following Virtualization software packages:

- VMware®:
  - Virtualization platform: VSphere 6.0, vSphere 6.5
  - High Availability & Fault-tolerant software:

    ESXi 6.0 (build 3620759) managed by VCenter Server Appliance v6.0.0 (build 3634788)

    ESXi 6.5 (build 5146846) managed by VCenter Server Appliance v6.5.0 (build 5318154)
- Stratus®:
  - Virtualization platform: KVM for Linux CentOS v7.0
  - High Availability & Fault-tolerant software: EverRun Enterprise 7.4.1
- Microsoft HyperV 2016:
  - Virtualization platform: Microsoft HyperV 2016
  - High Availability software: Microsoft HyperV Server 2016 v10.0.14393

**UL/ULC Deployments**
Supported virtualization software in UL/ULC deployments may differ from the ones mentioned before.

## 3.4.3 Microsoft SQL Server

Microsoft SQL Server 20014 R2 Express is free and included on the product DVD. Additional supported SQL version and editions are:

- Microsoft® SQL Server 2012 (Express, Standard and Enterprise)
- Microsoft® SQL Server 2014 (Express, Standard and Enterprise)
- Microsoft® SQL Server 2016 (Express, Standard and Enterprise)

**NOTE:**
Microsoft® SQL Server 2008 is no longer supported with Design CC V3.0.

## 3.4.4 Microsoft Office

Desigo CC uses Excel formats (xls, csv) for various purposes in the system. For example to import data point configuration, export values from Trends and Reports application, export OPC Server configuration, display Office documents in Document Viewer or as Link in Related Item, etc. The following versions and editions are supported:

- Microsoft® Office 2016 (Standard, Small Business, Professional, Enterprise)
- Microsoft® Office 2013 (Standard, Small Business, Professional, Enterprise)
- Microsoft® Office 2010 (Standard, Small Business, Professional, Enterprise)
- Microsoft® Office 2007 (Standard, Small Business, Professional, Enterprise)

## 3.4.5 Virus Scanners

Desigo CC Server, FEP, and Installed Clients are compatible with the following virus scanners:

- Kaspersky (© 1997-2017 Kaspersky Lab)
- Avira (© 2017 Avira Operations GmbH & Co. KG.)
- McAfee (© Copyright 2017 McAfee, LLC)
- Bitdefender (Copyright © 1997-2017 Bitdefender)
- TrendMicro Office Scan (Copyright 1998-2017 TrendMicro Inc.)
- AVG (Copyright © 2017 Avast Software)

## 3.4.6 Firewalls

Desigo CC Server, FEP, and Installed Clients are compatible with the following firewalls:

- Norton™ Security (©1995-2015 Symantec Corporation)
- Comodo Firewall (© 2015. Comodo Group, Inc.)
- Kaspersky TOTAL Security (© 1997-2017Kaspersky Lab)
- Bitdefender® Total Security (Copyright © 1997-2017 Bitdefender)
- McAfee End Point Security (© 2017 McAfee, Inc.)
- ZoneAlarm (ZoneAlarm® 2015 Extreme Security)
- Dell SonicWALL security (© 2015 SonicWALL L.L.C.)
- Check Point Next Generation Firewalls (©2015 Check Point Software Technologies Ltd.)
- Cisco PIX Firewall Software

### 3.4.7 PDF Readers

Desigo CC uses PDF documents for various purposes in the system. For example to create PDFs from Trends and Reports or display PDF documents in Document Viewer or as Link in Related Items, etc. The following readers are supported:

- PDF-XChange Viewer
- Adobe Reader (Copyright © 2017 Adobe Systems Incorporated)
- Foxit Reader (© 2015 Foxit Software Incorporated)
- CoolPDF (© Copyright 2000-2015 CoolPDF Software, Inc.)

### 3.4.8 AutoCAD Files

Desigo CC imports AutoCAD files, to be used as floor plans or background drawings in Graphics. The AutoCAD import formats up to version 2017 are supported:

- DWG
- DXF

## 3.5 Supported Subsystems and Standard Field Network Protocols Compatibility

Desigo CC is compatible with the following subsystems and protocols:

#### Building Automation

- APOGEE BACnet PXC, MBC, MEC controllers (firmware 3.2.4- 3.5)
- APOGEE BACnet FLN DXR, PTEC, PXC UEC, PPM
- APOGEE P2 PXC, MBC, MEC controllers P2 Ethernet (firmware 2.8.10) and RS-485 via AEM (firmware 2.8)
- APOGEE P1 FLN TEC, Point Expansion Modules, PXC Compact on P1, P1 BIM, DEM, P1 Drivers, and P1 VFDs
- Talon BACnet TC controllers (firmware 3.2.4-3.5)
- Desigo V5.1 Service Pack, V6.0, V6.1
- Desigo PX controllers (firmware ≥ 2.37)
- SIMATIC S7-300 /400 /1200* /1500* (* in compatibility mode)
- SICLIMAT X engineered S7-300 /400
- Climatix 600 range AHU HQ and district heating HQ: POL63… and POL68...(firmware versions as documented in online Help)

#### Third-party building automation systems using standard protocols Fire Safety

- Algorex EP7
- Algorex/Synova in a C-bus and Cerloop network (via NK823x)
- Desigo Fire Safety FS20 UL systems (FS20 UL MP1.x, MP2.0, MP2.1, MP2.2)
- Desigo Fire Safety Modular MP1.0
- FireFinder XLS (MP8, MP10, MP11, MP12)
- MXL (35.06J)

- Sinteso FS20 DE/EN (MP5.2 and MP6.0)
- Cerberus PRO CN (FS20-CN MP2.0: FC726, FC726-GQ)
- STT20 Centralisateur de Mise en Sécurité Incendie
- STT11/STT20 in a Cerloop network (via NK823x)
- Fibrolaser III OTS3 series controllers (direct via Modbus or via S4S OPC Server converter)
- DF8000 I/O System (via NK823x)
- Third-party fire systems using standard protocols:
- Honeywell Notifier ID3000 / ID3002 / ID50 / ID60 (via Modbus Intesis box converter v42.0.8)
- Aguilera AE/SA-C2, AE/SA-C8, AE/SA-C23H and AE/SA-C83H (via AE/SA-GAT interface version AGE48 2.0)
- Advantronic AD300 (via Modbus)
- Sensitron Multiscan ++ (v1.6.11 via Modbus)
- Sensitron Galileo (v2.21 via Modbus)

## Security

Video:

- Siveillance VMS200 embedded
- Siveillance VMS100
- Siveillance VMS200
- Siveillance VMS300
- Milestone XProtect Expert
- Milestone XProtect Corporate
- versions supported:
  2014 (7.0d), 2016 R3 SP1 (10.2b) and 2017 R1 (11.1a)

Access control:

- SiPass integrated 2.7 (with direct interface with SiPass removing the need of SX-API external gateway)
- SiPass integrated 2.65 is no longer supported in Desigo CC
- Third-party access systems using standard protocols:
- Selesta VAM Access Control System (via Selesta VAM OPC server v2.09)

Intrusion:

- SPC 3.4, 3.6.5, 3.6.6 (via EDP or FlexC protocol)
- SPC 3.7.1 (via FlexC protocol)
- Sintony F8-04, F8-05, F8-07, F9-22, G1 via NK823x

Third-party security systems using standard protocols, see the Intercom systems below:

- Third-party intercom systems using standard protocols
- TOA SOS Intercom Systems NS8000 (via S4S OPC server converter v1.0.0.3)

### Standard Protocols

- **BACnet**: Building Automation Control network, Revision 1.13
- **OPC Client:** OLE for Process Control OPC DA 2.05, 3.0
- **ONVIF**: Standard for IP video camera systems by Siveillance VMS
- **Modbus TCP:** Modbus IP communication protocol
- **SNMP:** SNMP Agents monitoring (V1 and V2)
- **IEC 61850: protocol for electrical substations and devices**

### Notification Protocols and Devices

- **Email**: POP3/IMAP/SMTP with SSL/TSL
- **Pager:** ESPA 4.4.4; Ascom
- **Mobile:** SMS
- **3G GSM Modem:**

  EHS6T USB modem from Gemalto

  HT63E, HT910E and HT910G modems from Telic
- **2G GSM Modem:**

  Siemens TC35i

  Siemens MC35i

  Cinterion MC52iT

  BGS5T, BGS2T and CT63 E modems from Gemalto

  GT864E modem from Telic

## 3.6 Supported Languages

Desigo CC software is delivered in English and can be extended with three additional languages. Following software language packages are available:

- Arabic
- Chinese (simplified)
- Chinese (traditional)
- Czech
- Danish
- Dutch
- English
- Finnish
- French
- German
- Hebrew
- Hungarian
- Italian
- Korean
- Norwegian
- Polish
- Portuguese
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
- Turkish
- Japanese

The Desigo CC Mass Notification extension module UI supports currently English and German only. Upon request, localization to other languages can be done.

# 3.7 Hardware Category Definitions

## 3.7.1 Physical Machines

| | AA | A | B | B1 | C | C1 | D | D1 |
|---|---|---|---|---|---|---|---|---|
| **CPU** | 1.83-2.0 GHz<br>Example:<br>Intel CeleronN2930<br>Intel Celeron 4C J1900 | 3.2 GHz<br>Core i5 or i7<br>4 cores<br>Example:<br>Intel Core i5 6600<br>Intel Core i5 7500 | 3.5 GHz<br>Core i7<br>4 cores<br>Example:<br>Intel Core i5 4690K<br>Intel Core i5 7600K | 3.5 Ghz<br>Core i7 or Xeon<br>6 cores<br>Example:<br>Xeon E5 1620v4<br>Xeon E5 1650v4 | 3.5-3.9 GHzCore i7 or Xeon6 coresExample:<br>Intel Core i7-4770K<br>Intel Core i77700<br>Intel Xeon E5-2643v4<br>Intel Xeon E5-1630 v4 | 2 x Phys. Processors(4 x vCPU) 3.5-3.9 GHz<br>Core i7 or Xeon<br>2 x 6 cores<br>Example:<br>2 x Intel Core i7-4770K<br>2 x Intel Xeon E5-2643v4 | 3.5-4.5 GHz<br>Core i7 or Xeon<br>8 cores<br>Example:<br>Intel Core i7 7700K<br>Intel Xeon E5-2667v4 | 2 x Phys. Processors(4 x vCPU) 3.5-4.5GHz<br>Core i7 or Xeon<br>2 x 8 cores<br>Example:<br>2 x Intel Core i7 7700K<br>2 x Intel Xeon E5-2667v4 |
| **RAM** | 8 GB | 8 GB | 16 GB | 32 GB | 32 GB | 64 GB | 32 GB | 64 GB |
| **Hard disk** | Size: 64 GB SSD | Size: 1 TB<br>RPM: 7.2k<br>Cache 64 MB | Size: 256 GB SSD +<br>1 TB RPM: 7.2k<br>Cache 64 MB | Size: 256 GB SSD +<br>2 x 1 TB RPM: 7.2k<br>Cache 64 MB | Size: 256 GB SSD +<br>2 x 1 TB RPM: 7.2k<br>Cache 64 MB | Size: 256 GB SSD +<br>2 x 1 TB RPM: 7.2k<br>Cache 64 MB | Size: 400 GB Enterprise SSD Mix Use | Size: 2 x 400 GB Enterprise SSD Mix Use |
| **Network card** | Gigabit speed | Gigabit speed | Gigabit speed | 2 x Gigabit speed | 2 x Gigabit speed | 2 x Gigabit speed | 2 x Gigabit speed | 2 x Gigabit speed |
| **Graphic card** | Onboard | Memory: 2 GB<br>Resolution: 2.560x1600<br>Example:<br>Onboard Intel 4600HD<br>AMD FirePro | Memory: 4 GB<br>Resolution: 2.560x1600<br>Example:<br>NVIDIA Quadro K1200<br>NVIDIA Quadro | Memory: 4GB<br>Resolution: 2.560x1600<br>Example:<br>NVIDIA Quadro K1200<br>NVIDIA Quadro | Onboard | Onboard | Onboard | Onboard |

| | AA | A | B | B1 | C | C1 | D | D1 |
|---|---|---|---|---|---|---|---|---|
| | | W2100 | K2200 | K2200 | | | | |
| **Monitor** | Size: 24'', Full HD, Resolution: 1920x1080 | Size: 24'', Full HD, Resolution: 1920x1080 | Size: 24'', Full HD, Resolution: 1920x1080 | Size: 24'', Full HD, Resolution: 1920x1080 | Size: 24'', Full HD, Resolution: 1920x1080 | Size: 24'', Full HD, Resolution: 1920x1080 | Size: 24'', Full HD, Resolution: 1920x1080 | Size: 24'', Full HD, Resolution: 1920x1080 |
| **Use for Server** | Up to 10,000 system objects and only in embedded Windows PC with Win10 IOT Enterprise 2016 LTSB version | Up to 25,000 system objects | Up to 50,000 system objects | Up to 50,000 system objects | Up to 100,000 system objects | Up to 100,000 system objects | Up to 150,000 system objects | Up to 150,000 system objects |
| **Use for Clients** | No | Yes | Yes | Yes | No | No | No | No |
| **Use for FEP** | No | Yes | Yes | Yes | Yes | No | No | No |
| **Use for Remote Web Server** | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| **Use for Remote SQL Server** | No | No | No | Yes | Yes | Yes | No | No |
| **Use for distribution** | No | No | No | Yes | No | Yes | No | Yes |
| **Use for virtualization** | No | No | No | No | No | Yes | No | Yes |
| **Use for Mass Notification** | No | Yes<br>Up to 50 audio zones | Yes<br>Up to 50 audio zones | Yes<br>Up to 100 audio zones | Yes<br>Up to 100 audio zones | Yes<br>Up to 100 audio zones with 6 vCPUs | Yes<br>Up to 150 audio zones | Yes<br>Up to 150 audio zones with 8 vCPUs |

**NOTE:**
Typically customer installations are very vital over the whole lifecycle. We recommend providing for reserves for the future and consider a higher hardware category than originally designed.

**NOTE:**
Showing Multiple Video streams at high performance and resolutions and graphics simultaneously requires a gaming graphic card at the Client (Example: GeForce GTX 970 Gaming 4G or equivalent)

**NOTE:**
The recommendations provided here are based on tests executed on hardware products available at the time of current Desigo CC version release.
Compatibility and performances using other software and hardware that might become current at some future point cannot be guaranteed. In such cases, please contact your local support for further information.
Standard hardware configurations defined above are available to Siemens SSP / CPS organizations. Please contact your local procurement manager for further information.

**NOTE:**
UL/ULC Compliance
For UL/ULC compliance, all computers in the system (Server, Clients and FEP) must be UL864 listed (Comark computer). Refer to section 3.7.3 for UL/ULC computer information.

**NOTE:**
In case of using a remote SQL Server, required hard disk space for categories A and B can go down to 500 GB.

**NOTE:**
Hardware Category AA can be used only in embedded hardware as mentioned above. The tests where it has been proved to work have been using the Desigo CC compact product for BA.. In standard hardware configurations category A is the minimum hardware category where Design CC can be installed, with the limits specified above

### 3.7.2 Physical Machines (with MNS)

For Desigo CC projects with MNS, the number of logical cores is also important, for its performance. 1 physical CPU core corresponds to 2 logical CPU cores. In addition to the standard HW categories A, B, C, D mentioned above, the following 3 categories have to be considered.

- B1 = Class B, CPU with at least 6 logical cores
- C1 = Class C, CPU with at least 2x6 logical cores
- D1 = Class D, CPU with at least 2x8 logical cores

| **Objects /<br>Mass Notification Size** | **0..25,000** | **25,001 .. 50,000** | **50,001..100,000** | **100,001..150,000** |
|---|---|---|---|---|
| **Small** | Class A | Class B | Class C | Class D |
| **Medium** | B1 | B1 | D1 | D1 |
| **Large** | C1 | C1 | D1 | D1 |

For customers who need a UL/ULC Listed Server to run Fire safety on a Desigo CC and want to add MNS to the same Server, the Comark CPUs mentioned below (see also the second chapter below) are categorized as C1 resp. B1.

- DCC-W7I7-22L-S or DCC-W7I7-42L corresponds to a C1
- DCC-W7XN-22L-S or DCC-W7XN-42L-S correspond to B1
- For other needs, please contact Product Management or Technical Support

The definition of small, medium and large MNS projects can be found in section 3.2.1

### 3.7.3 Virtual Machines

| Hardware Categories for Desigo CC - Virtual Machines | | | | |
|---|---|---|---|---|
| Category | A | B | C | D |
| vCPU | 2 | 2 | 2 | 4 |
| Memory | 8 GB | 16 GB | 32 GB | 32 GB |
| Hard Disk | Size: 1 TB | Size: 1 TB | Size: 2 TB | Size: 2 TB |
| Network Card | Gigabit speed | Gigabit speed | Gigabit speed | Gigabit speed |
| Use for Server | Up to 25,000 system objects | Up to 50,000 system objects | Up to 100,000 system objects | Up to 150,000 system objects |
| Use for Clients | No | No | No | No |
| Use for FEP | Yes | Yes | Yes | Yes |
| Use for Remote Web Server | Yes | Yes | Yes | Yes |
| Use for Remote SQL Server | Yes | Yes | Yes | Yes |
| Use for Distribution | No | Yes ( with 32 GB RAM) | Yes (with 64 GB RAM, host 96 GB RAM minimum) | Yes (with 64 GB RAM, host 96 GB RAM minimum) |

NOTE:
Refer to the visualization software specifications to indicate the hardware requirements for the Virtual Machine hosts.

### Hardware Categories for Desigo CC - Virtual Machines

**NOTE:**
UL/ULC Compliance
For UL/ULC compliance, all computers in the system (Server, Clients and FEP) must be UL/ULC listed (Comark computer). The use of virtual machines is not UL/ULC compliant. Refer to section 3.7.3 for UL/ULC computer information.

**NOTE:**
In case of remote SQL Server, the required hard disk space for categories A and B can go down to 500 GB.

For Desigo CC projects with the EM MNS, take also into consideration chapter 0

## 3.7.4 UL/ULC Listed Machines

The following table provides a mapping of the Desigo CC Hardware Categories to the available UL/ULC listed computers. After determining the required Hardware Category with the System Dimensioning Guide Calculator, the appropriate UL/ULC listed computer model number(s) can be determined by locating the corresponding Hardware Category in the table below.

The UL/ULC computers are sold as a Hardware/Software Server Package for small to medium sized systems (Hardware Category B) or as Hardware Only as defined below.

**Hardware/Software Package**

- UL/ULC listed Hardware Category B computer
- Choice of 22” or 42” LCD monitor
- Desigo CC software installed w/ Fire extension modules (EM)
  - Configured as a Desigo CC Server + Client
- Windows 10 operating system
- SNC card for XNET connection
- Desigo CC DVD (Software licenses not included)

**Hardware Only**

- UL/ULC listed computer
- Monitor ordered separately
- Desigo CC software is not installed
- Operating system
  - Windows 10 Professional or Server 2012 R2 depending on Hardware Category
- SNC card for XNET connection
- No Desigo CC DVD

Refer to the Desigo CC V3.0 Delivery Release for detailed ordering information.

| Desigo CC – UL / ULC Listed Machines | | | | |
|---|---|---|---|---|
| Category | A | B | C | D |
| Model Numbers for Hardware / Software Server Package | N/A | DCC-CATB-PKG-SM<br>– OR –<br>DCC-CATB-PKG-LM | N/A | N/A |
| Model Numbers for Hardware Only | UHW-CATA-01 | UHW-CATB-01 | UHW-CATC-01 | UHW-CATD-01 |

**NOTE:**
The Hardware Only computers can be used for Server, Client, or Front End Processor (FEP) configurations as indicated in Section 3.7.1, Physical Machine (without MNS).

# 3.8 Hardening Guidelines for Desigo CC Deployments

This section defines the minimal hardening measures that must be applied for each of the reference deployments in order to comply with Desigo CC requirements, and therefore meet Security Level 1 (SL1).

## 3.8.1 D1: Unsecured Desktop

IT Security Level 1 for Desigo CC cannot be achieved at this level of hardening. Therefore, do not use without an express written waiver of responsibility by the customer.

| Measures or Description | |
|---|---|
| Location of the physical server | On desktop where access by uncontrolled persons is possible |
| Physical/virtual server exclusivity | Non-exclusive: a computer also used for normal office tasks, including private surfing on the Internet |
| Physical server protective measures | None |
| Server protective measures (Software) | Standard antivirus and standard desktop firewall configuration (auto allowance ON), maintained. |
| Server OS version and set up | Off-the-shelf Windows installation |
| Client OS version and set up | N/A |
| Client protective measures (Software) | N/A |
| Connection for clients inside the customer network | N/A |
| Connection for clients outside the customer network (Remote access) | N/A |
| Remote access | Via remote desktop |
| Printers connectivity | Yes |
| IT skills of users | Low |
| IT skills of system administrators | Low |
| IT skills of network administrators | Low |
| IT skills of the installer (BT or VAP) | Low |
| Field devices connectivity | Directly on the customer network |
| Connection to other services (for example, OPC servers and clients) | Directly on the customer network |
| Client Windows login | Administrative auto-logon |
| Desigo CC users | Desigo CC authentication |
| Desigo CC client options | Any client option |

## 3.8.2 D2: Stand-alone Desktop Application

### Applicability

| | |
|---|---|
| Location of the physical server | On the desktop of one of the users in a controlled office environment (not in a publicly accessible area). |
| Physical/virtual server exclusivity | Non-exclusive: a computer also used for regular office tasks. |

| Topic | Required Hardening |
|---|---|
| Physical server protective measures | Unplug and theft protection. |
| Server protective measures (Software) | Disable interfaces with memory access (FireWire, USB 3.1).<br>Encrypt the hard disk.<br>Continuously maintained and strong antivirus protection.<br>Continuously maintained desktop firewalls.<br>Firewalls rules not on auto allowance, UPS needed. |
| Server OS version and set up | Secure Windows OS installation.<br>Set up and maintain Windows OS security.<br>Keep Windows OS continuously updated by security patches.<br>Enforce strong password policy.<br>Restrict access to users and to Desigo CC applications. |
| Client OS version and set up | N/A |
| Client protective measures (Software) | N/A |
| Connection for clients inside the customer network | N/A |
| Connection for clients outside the customer network (Remote access) | N/A |
| Remote access | Via remote desktop |
| Printers connectivity | Yes |
| IT skills of users | Low |
| IT skills of system administrators | Medium |
| IT skills of network administrators | Medium |
| IT skills of the installer (BT or VAP) | Medium |
| Field devices connectivity | Directly, via V-LAN or customer networks: customer is responsible for securing it. The assumption is that the customer’s IT secures field device connectivity. |
| Connection to other services (for example: OPC servers and clients) | Directly, via V-LAN or customer networks: customer is responsible for securing it. The assumption is that the customer’s IT secures field device connectivity. |
| Client Windows login | No auto-logon or professional KIOSK mode. |
| Desigo CC users | Use Windows authentication only. |
| Desigo CC client options | Any client option. |

## 3.8.3 D3: Client/Server Application in Office Environment

### Applicability

| | |
|---|---|
| Location of the physical server | On the desktop of one of the users in a controlled office environment (not in a publicly accessible area). |
| Physical/virtual server exclusivity | Non-exclusive: a computer also used for regular office tasks. |

| Topic | Required Hardening |
|---|---|
| Physical server protective measures | Unplug and theft protection |
| Server protective measures (Software) | Disable interfaces with memory access (FireWire, USB 3.1).<br>Encrypt the hard disk.<br>Continuously maintained and strong antivirus protection.<br>Continuously maintained desktop firewalls.<br>Firewalls rules not on auto allowance, UPS needed, FEP in enclosed environment (locked cabinet). |
| Server OS version and set up | Secure Windows OS installation.<br>Set up and maintain Windows security.<br>Keep Windows OS continuously updated by security patches.<br>Enforce strong password policy.<br>Restrict access to users and to Desigo CC applications.<br>Secured network configuration (for example, managed access rights to network folders). |
| Client OS version and set up | Secure Windows OS installation.<br>Set up and maintain Windows security<br>Keep Windows OS continuously updated by security patches.<br>Enforce strong password policy<br>Restrict access to users and to Desigo CC applications<br>Managed certificates and credential |
| Client protective measures (Software) | Disable interfaces with memory access (FireWire, USB 3.1).<br>Continuously maintained and strong antivirus protection.<br>Continuously maintained desktop firewalls.<br>Firewalls rules not on auto allowance.<br>Secure certificate store.<br>Set up all applications running on the client.<br>Do not store passwords locally |
| Connection for clients inside the customer network | Secured communication configured.<br>Segmented Network.<br>Network firewalls configured and continuously maintained. |
| Connection for clients outside the customer network (Remote access) | Secured communication configured.<br>Segmented Network.<br>Network firewalls configured and continuously |

| Topic | Required Hardening |
|---|---|
| | maintained.<br>DMZ configured. |
| Remote access | Via remote desktop and VPN.<br>Clients on Internet restricted to "need to know". |
| Printers connectivity | Yes |
| IT skills of users | Low |
| IT skills of system administrators | Medium |
| IT skills of network administrators | High |
| IT skills of the installer (BT or VAP) | Medium |
| Field devices connectivity | Directly, via V-LAN or customer networks: customer is responsible for securing it. The assumption is that the customer’s IT secures field device connectivity. |
| Connection to other services (for example, OPC servers and clients) | Directly, via V-LAN or customer networks: customer is responsible for securing it. The assumption is that the customer’s IT secures field device connectivity. |
| Client Windows login | No auto-logon or professional KIOSK mode. |
| Desigo CC users | Use Windows authentication only. |
| Desigo CC client-options | Use Windows App and Web Client only. |

## 3.8.4 D4: Client/Server Application in a Secured Location/Control Room

### Applicability

| | |
|---|---|
| Suitable and supported for IT security | If Desigo CC security prescriptions are applied |
| Location of the physical server | Supervised control room desk and enclosure |

| Topic | Required Hardening |
|---|---|
| Physical/virtual server exclusivity | Non-exclusive: a computer also used for regular office tasks. |
| Physical server protective measures | Server machine locked in cabinet.<br>Unplug and theft protection. |
| Server protective measures (Software) | Disable interfaces with memory access (FireWire, USB 3.1).<br>Encrypt the hard disk.<br>Continuously maintained and strong antivirus protection.<br>Continuously maintained desktop firewalls.<br>Firewalls rules not on auto allowance, UPS needed, FEP in enclosed environment (locked cabinet). |
| Server OS version and set up | Secure Windows OS installation.<br>Set up and maintain Windows security.<br>Keep Windows OS continuously updated by security patches.<br>Enforce strong password policy.<br>Restrict access to users and to Desigo CC applications.<br>Secured network configuration (for example, |

| Topic | Required Hardening |
|---|---|
| | managed access rights to network folders) |
| Client OS version and set up | Secure Windows OS installation.<br>Set up and maintain Windows security.<br>Keep Windows OS continuously updated by security patches.<br>Enforce strong password policy.<br>Restrict access to users and to Desigo CC applications.<br>Managed certificates and credentials. |
| Client protective measures (Software) | Disable interfaces with memory access (FireWire, USB 3.1).<br>Continuously maintained and strong antivirus protection.<br>Continuously maintained desktop firewalls.<br>Firewalls rules not on auto allowance.<br>Secure certificate store.<br>Set up all applications running on the client.<br>Do not store passwords locally. |
| Connection for clients inside the customer network | Secured communication configured.<br>Segmented Network.<br>Network firewalls configured and continuously maintained. |
| Connection for clients outside the customer network (Remote access) | Secured communication configured.<br>Segmented Network.<br>Network firewalls configured and continuously maintained.<br>DMZ configured. |
| Remote access | Via remote desktop and VPN.<br>Clients in Internet restricted to "need to know". |
| Printers connectivity | Yes |
| IT skills of users | Low |
| IT skills of system administrators | Medium |
| IT skills of network administrators | High |
| IT skills of the installer (BT or VAP) | Medium |
| Field devices connectivity | Directly, via V-LAN or customer networks: customer is responsible for securing it. The assumption is that the customer’s IT secures field device connectivity. |
| Connection to other services (for example: OPC servers and clients) | Directly, via V-LAN or customer networks: customer is responsible for securing it. The assumption is that the customer’s IT secures field device connectivity. |
| Client Windows login | No auto-logon or professional KIOSK mode. |
| Desigo CC users | Use Windows authentication only. |
| Desigo CC client options | Any client-option |

### 3.8.5 D5: Client/Server Application in a Professional IT Environment

#### Applicability

| | |
|---|---|
| Location of the physical server | Restricted server room |
| Physical/virtual server exclusivity | Exclusive: Server only hosts Desigo CC applications |

| Topic | Required Hardening |
|---|---|
| Physical server protective measures | Server machine locked in cabinet.<br>Unplug and theft protection. |
| Server protective measures (Software) | Disable interfaces with memory access (FireWire, USB 3.1).<br>Encrypt the hard disk.<br>Continuously maintained and strong antivirus protection.<br>Continuously maintained desktop firewalls.<br>Firewalls rules not on auto allowance, UPS needed, FEP in enclosed environment (locked cabinet). |
| Server OS version and set up | Patched secure Windows installation.<br>Set up and maintain Windows security.<br>Keep Windows OS continuously updated by security patches.<br>Enforce strong password policy.<br>Restrict access to users and to Desigo CC applications.<br>Secured network configuration (for example, managed access rights to network folders).<br>Advanced malware protection.<br>Automated backup. |
| Client OS version and set up | Secure Windows OS installation.<br>Set up and maintain Windows security-<br>Keep Windows OS continuously updated by security patches.<br>Enforce strong password policy.<br>Restrict access to users and to Desigo CC applications.<br>Managed certificates and credentials. |
| Client protective measures (Software) | Disable interfaces with memory access (FireWire, USB 3.1).<br>Continuously maintained and strong antivirus protection.<br>Continuously maintained desktop firewalls.<br>Firewalls rules not on auto allowance.<br>Secure certificate store.<br>Set up all applications running on the client.<br>Do not to store passwords locally. |
| Connection for clients inside the customer network | Secured communication configured.<br>Segmented Network.<br>Network firewalls configured and continuously maintained. |

| Topic | Required Hardening |
|---|---|
| Connection for clients outside the customer network (Remote access) | Secured communication configured.<br>Segmented Network.<br>Network firewalls configured and continuously maintained.<br>DMZ configured. |
| Remote access | Via remote desktop and VPN.<br>Clients in Internet restricted to "need to know" |
| Printers connectivity | Yes |
| IT skills of users | Low |
| IT skills of system administrators | High |
| IT skills of network administrators | High |
| IT skills of the installer (BT or VAP) | High |
| Field devices connectivity | Via V-LAN and secure routing: customer is responsible to securing it. The assumption is that the customer’s IT secures field device connectivity. |
| Connection to other services<br>(for example, OPC servers and clients) | Via V-LAN and secure routing: customer is responsible to securing it. The assumption is that the customer’s IT secures field device connectivity. |
| Client Windows login | Professionally secured KIOSK mode. |
| Desigo CC users | Use IDM/Kerberos authentication. |
| Desigo CC client-options | Use Windows App and Web Client only. |

# 4 Part C: Multi-discipline Configurations

## 4.1 Introduction

The following sections provide information for typical multi-discipline configurations (reference configurations). These are uses cases with typical numbers of data points for the different disciplines. These figures do not indicate the system limits.

| Use Case | Remarks |
|---|---|
| BAS & Video | · Building Automation System (BAS) with up to 50'000 System Objects<br>· Video with up to 1,000 cameras |
| BAS & Video & Access Control | · Building Automation System (BAS) with up to 50'000 System Objects<br>· Video with up to 1,000 cameras<br>· SiPass Access Control System with up to 1000 doors |
| BAS & Fire | EN and UL/ULC configurations:<br>· Building Automation System (BAS)<br>· Fire System (FS20, AlgoRex and XLS/MXL)<br>· Up to 60,000 System objects for BAS and Fire |
| BAS & Fire & Video | EN and UL/ULC configurations:<br>· Building Automation System (BAS)<br>· Fire System (FS20, AlgoRex and XLS/MXL)<br>· Up to 60,000 System objects for BAS and Fire<br>· Video with up to 1,000 (EN) / 128 (UL/ULC) cameras |
| BAS & MNS | · Building Automation System (BAS) with up to 50,000 System Objects<br>· MNS: Multiple notification recipients as e.g. SMS, Pager, IP Phones, E-mail, PC, LED signs, loudspeaker, Facebook … |
| MNS & Video | · Video with up to 1,000 cameras<br>· MNS: Multiple notification recipients as e.g. SMS, Pager, IP Phones, E-mail, PC, LED signs, loudspeaker, Facebook … |
| Fire & Video | EN and UL/ULC configurations:<br>· Fire System (FS20, AlgoRex and XLS/MXL)<br>· Up to 50,000 System objects for Fire<br>· Video with up to 1,000 (EN) / 128 (UL/ULC) cameras |
| DMS | EN configurations:<br>· Fire System (FS20 and AlgoRex)<br>· Intrusion System (SPC and Sintony)<br>· Up to 50,000 System objects for Fire and Intrusion<br>· Video with up to 1,000 cameras<br>· SiPass Access Control System with up to 1,000 doors |
| Fire & MNS | UL/ULC and non UL/ULC configurations:<br>· Fire System (FS20, AlgoRex and XLS/MXL)<br>· Up to 50,000 System objects for Fire<br>· MNS: E-Mail notifications (UL/ULC) or multiple notification recipients as e.g. SMS, Pager, IP Phones, E-mail, PC, LED signs, loudspeaker, Facebook …(EN) |
| BAS & Fire & MNS | · Building Automation System (BAS)<br>· Fire System (FS20, AlgoRex and XLS/MXL)<br>· Up to 60,000 System objects for BAS and Fire<br>· MNS: E-Mail notifications (UL/ULC) or multiple notification recipients as e.g. SMS, Pager, IP Phones, E-mail, PC, LED signs, loudspeaker, Facebook…(EN) |

| Use Case | Remarks |
|---|---|
| TBS & Fire Monitoring-Only | · Non UL/ULC TBS System with Desigo CC management platform<br>· UL/ULC Fire System (XLS/MXL and/or FS20) |

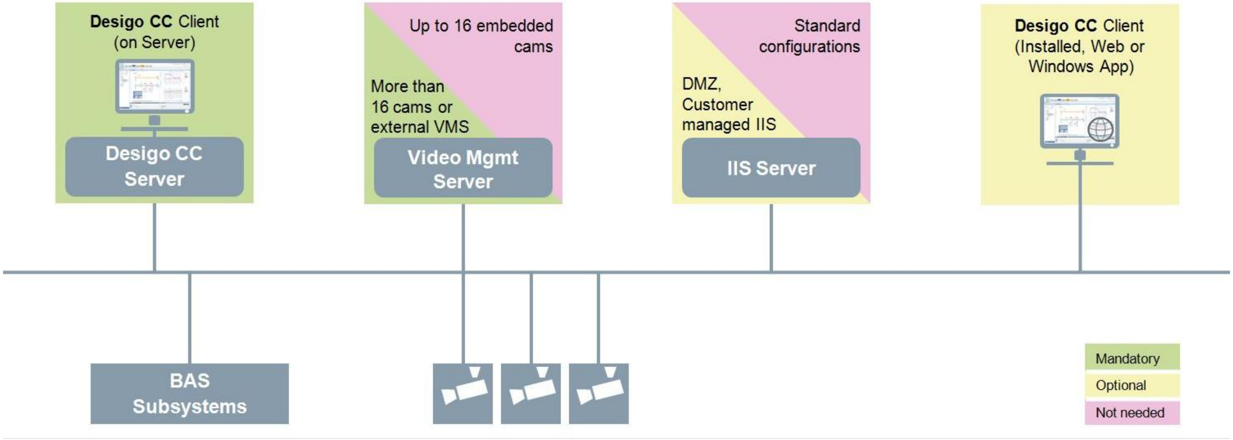
**NOTE:**
The following sections provide recommendations based on average system configurations. The dimensioning tool has to be used for details and will provide hardware recommendations for other configurations with different numbers of data points.

## 4.2 BAS and Video

Configuration Description:

- Building Automation System (BAS) with up to 50,000 System Objects (see dimensioning tool)
- Video with up to 1000 cameras

Topology:


Desigo CC Client (on Server)
Desigo CC Server
Up to 16 embedded cams
More than 16 cams or external VMS
Video Mgmt Server
Standard configurations
DMZ, Customer managed IIS
IIS Server
Desigo CC Client (Installed, Web or Windows App)
BAS Subsystems
Mandatory
Optional
Not needed

Required Hardware:

| PC | Role | Specification | Comments |
|---|---|---|---|
| DCC Server | Mandatory, needed for:<br>· BAS integration<br>· DCC Client<br>· Video driver<br>· Video Server (for up to 16 embedded cams)<br>· (IIS Server) | PC HW Cat C | Single PC deployment possible for configurations with up to 16 cameras.<br>If >16 cameras: Video Server requires dedicated PC (see below)<br>**Note:** up to 16 video streams on client |
| FEPs | Not needed | | |
| Clients | Optional additional client | PC HW Cat A | Total number of clients is limited to:<br>· 10 Installed Clients<br>· 27 Windows App or Web Clients<br>· 2 if embedded video on DCC server<br>· 20 if embedded video with Video Server<br>· 25 if external VMS<br>That means:<br>· Up to 9 additional Installed Clients<br>· Up to 24 additional Windows App or Web Clients<br>**Note:** up to 16 video streams per client |
| Mobile App | Optional mobile app client | | Up to 10/100 mobile app clients |

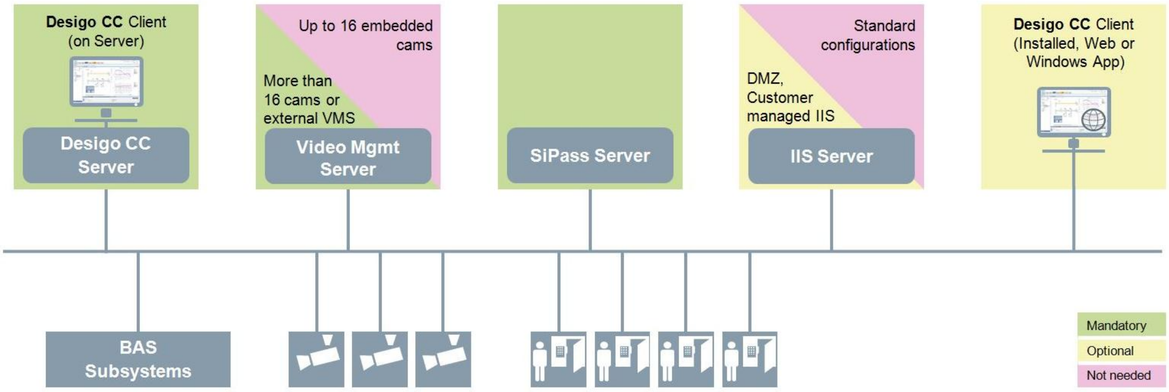
| PC | Role | Specification | Comments |
|---|---|---|---|
| Clients | | | (see section 4.12, Remarks) |
| Dedicated Video Server | Not needed for up to 16 embedded cams | | |
| | Mandatory, if<br>>16 embedded cams or for external VMS | See Milestone/ Siveillance VMS | VMS software (embedded or external) has to be installed on this PC |
| SiPass Server | Not needed | | |
| Dedicated IIS Server | Not needed for standard configurations | | |
| | Recommended for configurations with:<br>· DMZ<br>· Customer managed IIS | PC HW Cat A | |
| Dedicated SQL Server | Not needed | | |

## 4.3 BAS, Video and Access Control

Configuration Description:

- Building Automation System (BAS) with up to 50,000 System Objects (see dimensioning tool)
- Video with up to 1,000 cameras
- SiPass Access Control System with up to 1,000 doors

Topology:



Required Hardware:

| PC | Role | Specification | Comments |
|---|---|---|---|
| DCC Server | Mandatory, needed for:<br>· BAS integration<br>· SiPass integration (via BACnet)<br>· DCC Client<br>· Video driver<br>· Video Server (for up to 16 embedded cams)<br>· (IIS Server) | PC HW Cat C | If >16 cameras: Video Server requires dedicated PC (see below)<br>**Note:** up to 16 video streams on client |
| FEPs | Not needed | | |
| Clients | Optional additional client | PC HW Cat A | Total number of clients is limited to:<br>· 10 Installed Clients<br>· 27 Windows App or Web Clients<br>· 2 if embedded video on DCC server<br>· 20 if embedded video with Video Server<br>· 25 if external VMS<br>That means:<br>· Up to 9 additional Installed Clients<br>· Up to 24 additional Windows App or Web Clients |

| PC | Role | Specification | Comments |
|---|---|---|---|
| | | | **Note:** up to 16 video streams per client |
| Mobile App Clients | Optional mobile app client | | Up to 10/100 mobile app clients<br>(see section 4.12, Remarks) |
| Dedicated Video Server | Not needed for up to 16 embedded cams | | |
| | Mandatory, if<br>>16 embedded cams or for external VMS | See Milestone/ Siveillance VMS | VMS software (embedded or external) has to be installed on this PC |
| SiPass Server | Mandatory | PC HW Cat B | Runs SiPass Server (& Client) |
| Dedicated IIS Server | Not needed for standard configurations | | |
| | Recommended for configurations with:<br>· DMZ<br>· Customer managed IIS | PC HW Cat A | |
| Dedicated SQL Server | Not needed | | |

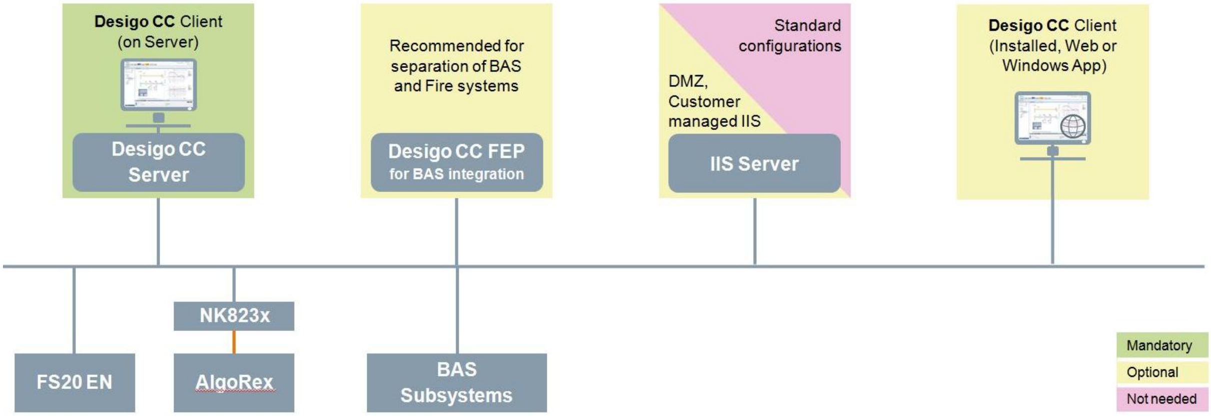
# 4.4 BAS and Fire

Configuration Description:

- Building Automation System (BAS)
- Fire System (FS20, AlgoRex and XLS/MXL)
- Up to 60,000 System objects for BAS and Fire (see dimensioning tool)

## 4.4.1 EN Configurations

Topology:


Desigo CC Client (on Server)
Desigo CC Server
Recommended for separation of BAS and Fire systems
Desigo CC FEP for BAS integration
Standard configurations
DMZ, Customer managed IIS
IIS Server
Desigo CC Client (Installed, Web or Windows App)
NK823x
FS20 EN
AlgoRex
BAS Subsystems
Mandatory
Optional
Not needed

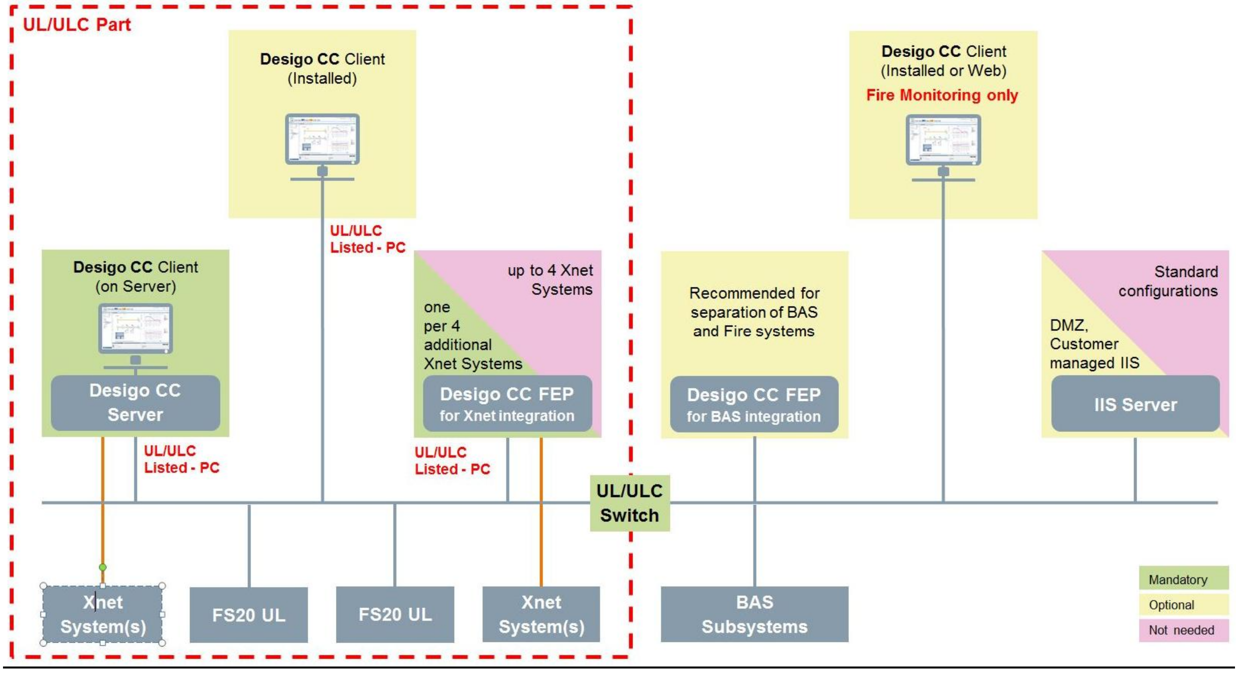
Required Hardware:

| PC | Role | Specification | Comments |
|---|---|---|---|
| DCC Server | Mandatory, needed for:<br>· Fire integration<br>· (BAS integration)<br>· DCC Client<br>· (IIS Server) | PC HW Cat C | FS20: Up to 64 nodes per driver<br>(see section 4.12, Remarks)<br>AlgoRex: Up to 4 C-Bus networks per driver (via NK823x)<br>Server: Up to 5 drivers in total |
| FEP 1 | Optional for BAS integration | PC HW Cat B | Dedicated FEP is recommended to separate the BAS from the Fire system.<br>**Note:** online/auto configuration not supported on FEP. |
| FEP 2 to 5 | Not needed | | |
| Clients | Optional additional client for:<br>· BAS operation<br>· Fire Control | PC HW Cat A | Total number of clients is limited to:<br>· 10 Installed Clients<br>· 27 Windows App or Web Clients<br>That means: |

| | | | |
|---|---|---|---|
| | | | · Up to 9 additional Installed Clients<br>· Up to 27 additional Windows App or Web Clients<br>Client could also be installed on FEPs |
| Mobile App Clients | Optional mobile app client for:<br>· BAS operation<br>· Fire Control | | Up to 10/100 mobile app clients (see section 4.12, Remarks) |
| Video Server | Not needed | | |
| SiPass Server | Not needed | | |
| Dedicated IIS Server | Not needed for standard configurations | | |
| | Recommended for configurations with:<br>· DMZ<br>· Customer managed IIS | PC HW Cat A | |
| Dedicated SQL Server | Not needed | | |
| Misc. | Ethernet Gateway for AlgoRex | NK823x | Up to 4 C-Bus networks per NK823x |

## 4.4.2 UL/ULC Configurations

Topology:



**Note:**

- In case the distance between DCC stations and fire panels within the UL/ULC part is less than 20ft, copper wires in conduit can be used; otherwise fiber optics with listed switches are required.

Required Hardware:

| PC | Role | Specification | Comments |
|---|---|---|---|
| DCC Server | Mandatory, needed for:<br>· Fire integration (via DMS/NCC-2F and/or BACnet)<br>· (BAS integration)<br>· DCC Client<br>· (IIS Server) | UL/ULC Listed - PC HW Cat C | XNET: Up to 4 XNET can be integrated. In case of more XNETs additional FEP's are required (see below)<br>FS20: Up to 64 nodes per driver (see section 4.12, Remarks)<br>Server: Up to 5 drivers in total |
| FEP 1 | Optional for BAS integration | PC HW Cat B | Dedicated FEP is recommended to separate the BAS from the Fire system.<br>**Note:** online/auto configuration not supported on FEP. |
| FEP 2 to5 | Required for additional XNET connection via DMS/NCC-2F | UL/ULC Listed - PC HW Cat B | One additional FEP per 4 additional XNET connections is required<br>Up to 4 FEPs for XNET are supported. |
| | Not needed for up to 1 XNET | | |
| Clients (UL/ULC) | Optional additional client for:<br>· Fire Control<br>· BAS operation | UL/ULC Listed - PC HW Cat A | Total number of clients (UL/ULC and non UL/ULC) is limited to:<br>· 7 Installed Clients<br>· 20 Web Clients<br>That means:<br>· Up to 6 additional Installed Clients<br>· Web Clients not allowed for fire control<br>Client could also be installed on FEP for XNET integration |
| Clients (non UL/ULC) | Optional additional client for:<br>· Fire Monitoring (no Control)<br>· BAS operation | PC HW Cat A | Total number of clients (UL/ULC and non UL/ULC) is limited to:<br>· 7 Installed Clients<br>· 20 Web Clients<br>That means:<br>· Up to 6 additional Installed Clients<br>· Up to 19 additional Web Clients (no Windows App Clients)<br>Client could also be installed on FEP for BAS integration |
| Mobile App Clients | Optional mobile app client for<br>· Fire Monitoring (no Control)<br>· BAS operation | | Up to 10 mobile app clients (see section 4.12, Remarks) |
| Dedicated Video Server | Not needed | | |
| SiPass Server | Not needed | | |
| Dedicated IIS Server | Not needed for standard configurations | | |
| | Recommended for configurations with:<br>· DMZ<br>· Customer managed IIS<br>· UL/ULC compliance | PC HW Cat A | |
| Dedicated SQL Server | Not needed | | |
| Misc. | UL/ULC switches | | |

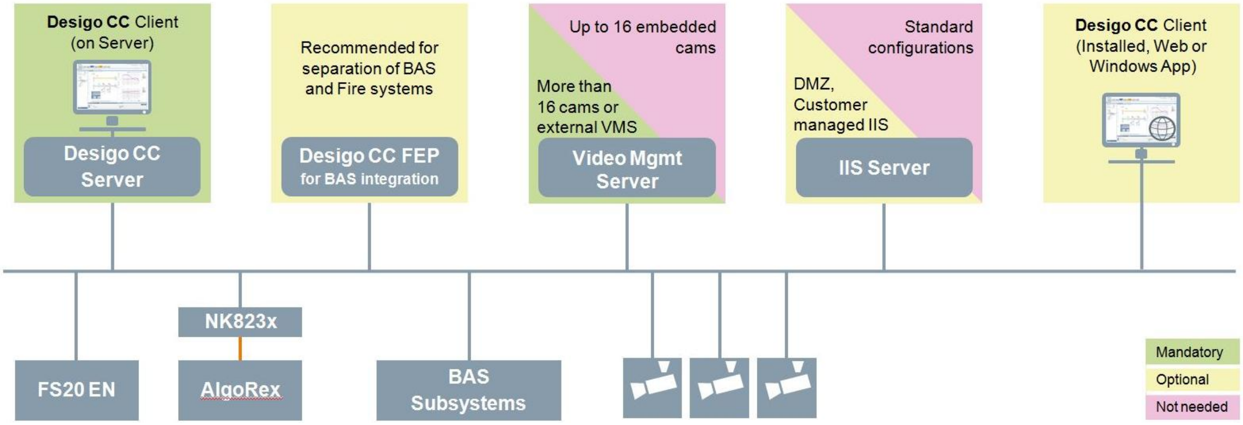
# 4.5 BAS, Fire and Video

Configuration Description:

- Building Automation System (BAS)
- Fire System (FS20, AlgoRex and XLS/MXL)
- Up to 60’000 System objects for BAS and Fire (see dimensioning tool)
- Video with up to 1,000 (EN) / 128 (UL/ULC) cameras

## 4.5.1 EN Configurations

Topology:

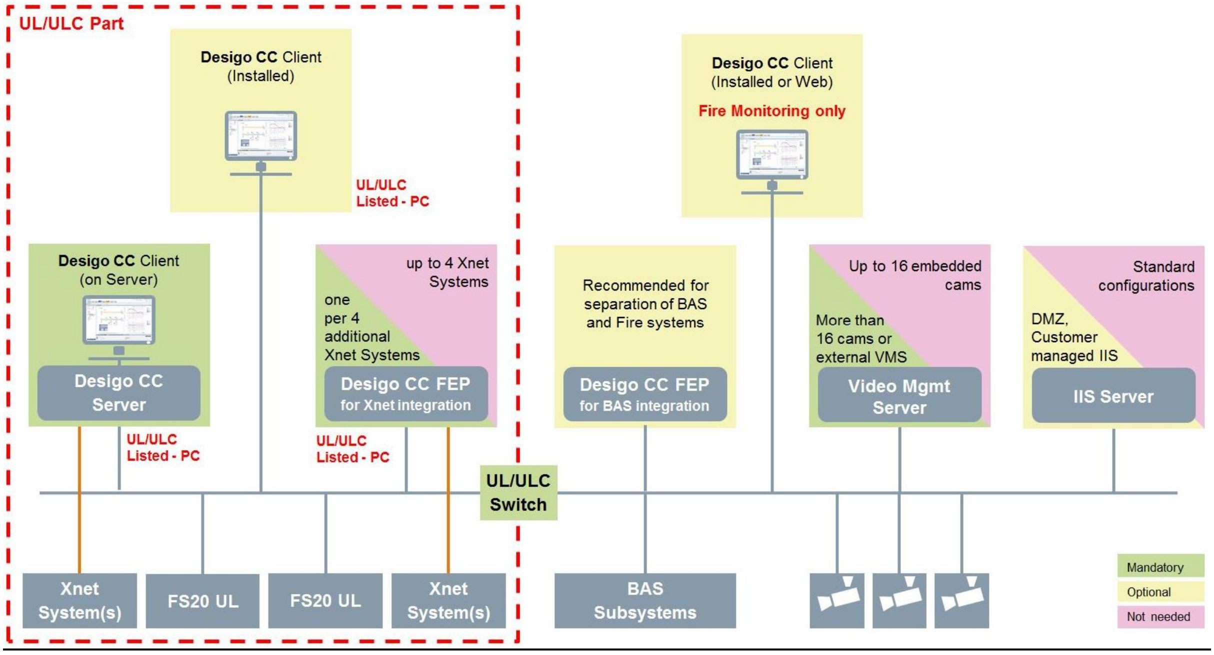

Desigo CC Client (on Server)
Desigo CC Server
Recommended for separation of BAS and Fire systems
Desigo CC FEP for BAS integration
Up to 16 embedded cams
More than 16 cams or external VMS
Video Mgmt Server
Standard configurations
DMZ, Customer managed IIS
IIS Server
Desigo CC Client (Installed, Web or Windows App)
FS20 EN
NK823x
AlgoRex
BAS Subsystems
Mandatory
Optional
Not needed

Required Hardware:

| PC | Role | Specification | Comments |
|---|---|---|---|
| DCC Server | Mandatory, needed for:<br>· Fire integration<br>· (BAS integration)<br>· DCC Client<br>· Video driver<br>· Video Server (for up to 16 embedded cameras)<br>· (IIS Server) | PC HW Cat C | FS20: Up to 64 nodes per driver (see section 4.12, Remarks)<br>AlgoRex: Up to 4 C-Bus networks per driver (via NK823x)<br>Video: If >16 cameras: Video Server requires dedicated PC (see below).<br>Up to 16 video streams on client.<br>Server: Up to 5 drivers in total |
| FEP 1 | Optional for BAS integration | PC HW Cat B | Dedicated FEP is recommended to separate the BAS from the Fire system.<br>**Note:** online/auto configuration not supported on FEP. |
| FEP 2 to 5 | Not needed | | |
| Clients | Optional additional client for:<br>· Video and BAS operation<br>· Fire Control | PC HW Cat A | Total number of clients is limited to:<br>· 10 Installed Clients<br>· 27 Windows App or Web Clients<br>· 2 if embedded video on DCC server<br>· 20 if embedded video with Video Server<br>· 25 if external VMS<br>That means:<br>· Up to 9 additional Installed Clients<br>· Up to 24 additional Windows App or Web Clients<br>**Note:** up to 16 video streams per client<br>Client could also be installed on FEPs |
| Mobile App Clients | Optional mobile app client for:<br>· BAS operation<br>· Fire Control | | Up to 10/100 mobile app clients (see section 4.12, Remarks) |
| Dedicated Video Server | Not needed for up to 16 embedded cams | | |
| | Mandatory, if<br>>16 embedded cams or for external VMS | See Milestone/ Siveillance VMS | VMS software (embedded or external) has to be installed on this PC |
| SiPass Server | Not needed | | |
| Dedicated IIS Server | Not needed for standard configurations | | |
| | Recommended for configurations with:<br>· DMZ<br>· Customer managed IIS | PC HW Cat A | |
| Dedicated SQL Server | Not needed | | |
| Misc. | Ethernet Gateway for AlgoRex | NK823x | Up to 4 C-Bus networks per NK823x |

## 4.5.2 UL/ULC Configurations

Topology:


UL/ULC Part
Desigo CC Client (Installed)
UL/ULC Listed - PC
Desigo CC Client (Installed or Web)
Fire Monitoring only
Desigo CC Client (on Server)
Desigo CC Server
UL/ULC Listed - PC
up to 4 Xnet Systems
one per 4 additional Xnet Systems
Desigo CC FEP for Xnet integration
UL/ULC Listed - PC
Recommended for separation of BAS and Fire systems
Desigo CC FEP for BAS integration
Up to 16 embedded cams
More than 16 cams or external VMS
Video Mgmt Server
Standard configurations
DMZ, Customer managed IIS
IIS Server
UL/ULC Switch
Xnet System(s)
FS20 UL
FS20 UL
Xnet System(s)
BAS Subsystems
Mandatory
Optional
Not needed

Remarks

- In case the distance amongst DCC stations and fire panels within the UL/ULC part is less than 20ft copper wires in conduit can be used, otherwise fiber optics with listed switches are required.
- A total of 2 clients is supported if the Video server runs on the Desigo CC Server.
- A total of 20 clients is supported for embedded Video with dedicated Video Server
- Video restriction for UL/ULC: up to 16 streams per client
  - 4x4 layout: 16 streams at max. CIF resolution (352x288) / 10FPS
  - 1+7 layout: 1 stream 4CIF(704x576) / 25FPS and 7 streams 2CIF (704x288) / 25FPS
  - 2x2 layout: 4 streams at max. 4CIF resolution (704x576) / 25FPS
  - 1 layout: 1 FullHD (1920x1080) / 30FPS

Required Hardware:

| PC | Role | Specification | Comments |
|---|---|---|---|
| DCC Server | Mandatory, needed for:<br>· Fire integration (via DMS/NCC-2F and/or BACnet)<br>· (BAS integration)<br>· DCC Client<br>· Video driver<br>· Video Server (for up to 16 embedded cameras)<br>· (IIS Server) | UL/ULC Listed - PC HW Cat C | XNET: Up to 4 XNET can be integrated. In case of more XNETs additional FEP's are required<br>FS20: Up to 64 nodes per driver (see remarks in section 4.12)<br>Video: If >16 cameras: Video Server requires dedicated PC.<br>Up to 16 video streams on client (with restrictions on video format)<br>Server: Up to 5 drivers in total |
| FEP 1 | Optional for BAS integration | PC HW Cat B | Dedicated FEP is recommended to separate the BAS from the Fire system.<br>**Note:** online/auto configuration not supported on FEP. |
| FEP 2 to 5 | Required for additional XNET connection via DMS/NCC-2F | UL/ULC Listed - PC HW Cat B | One additional FEP per 4 additional XNET connections is required<br>Up to 4 FEPs for XNET are supported. |

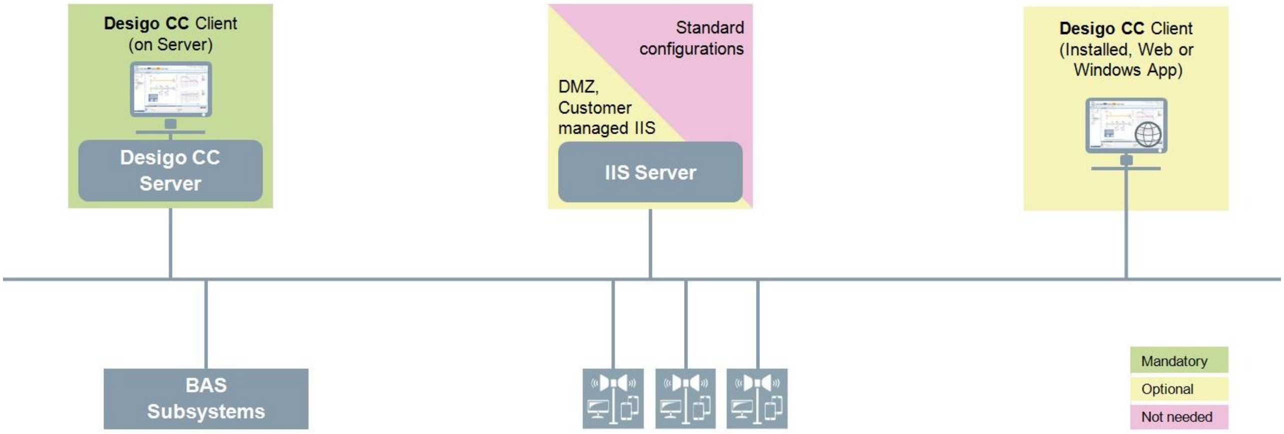
| PC | Role | Specification | Comments |
|---|---|---|---|
| | Not needed for up to 1 XNET | | |
| Clients (UL/ULC) | Optional additional client for:<br>· Fire Control<br>· Video and BAS operation | UL/ULC Listed - PC HW Cat A | Total number of clients (UL/ULC and non UL/ULC) is limited to:<br>· 7 Installed Clients<br>· 20 Web Clients<br>· 2 if embedded video on DCC server<br>· 20 if embedded video with Video Server<br>· 20 if external VMS<br><br>That means:<br>· Up to 6 additional Installed Clients<br>· Web Clients not allowed for fire control<br><br>**Note:** up to 16 video streams on client (with restrictions on video format)<br>Client could also be installed on FEP for XNET integration |
| Clients (non UL/ULC) | Optional additional client for:<br>· Fire Monitoring (no Control)<br>· Video and BAS operation | PC HW Cat A | Total number of clients (UL/ULC and non UL/ULC) is limited to:<br>· 7 Installed Clients<br>· 20 Web Clients<br>· 2 if embedded video on DCC server<br>· 20 if embedded video with Video Server<br>· 20 if external VMS<br><br>That means:<br>· Up to 6 additional Installed Clients<br>· Up to 19 additional Web Clients (no Windows App Clients)<br><br>**Note:** up to 16 video streams on client (with restrictions on video format)<br>Client could also be installed on FEP for BAS integration |
| Mobile App Clients | Optional mobile app client for<br>· Fire Monitoring (no Control)<br>· BAS operation | | Up to 10 mobile app clients<br>(see section 4.12, Remarks) |
| Dedicated Video Server | Not needed for up to 16 embedded cams | | |
| | Mandatory, if>16 embedded cams or for external VMS | See Milestone/ Siveillance VMS | VMS software (embedded or external) has to be installed on this PC |
| SiPass Server | Not needed | | |
| Dedicated IIS Server | Not needed for standard configurations | | |
| | Recommended for configurations with:<br>· DMZ<br>· Customer managed IIS<br>· UL/ULC compliance | PC HW Cat A | |
| SQL Server | Dedicated SQL Server not needed | | |
| Misc. | UL/ULC switches | | |

# 4.6 BAS and MNS

Configuration Description:

- Building Automation System (BAS) with up to 50,000 System Objects (see dimensioning tool)
- MNS: Multiple notification recipients as e.g. SMS, Pager, IP Phones, E-mail, PC, LED signs, loudspeaker, Facebook …

Topology:


Desigo CC Client (on Server)
Desigo CC Server
Standard configurations
DMZ, Customer managed IIS
IIS Server
Desigo CC Client (Installed, Web or Windows App)
BAS Subsystems
Mandatory
Optional
Not needed

Required Hardware:

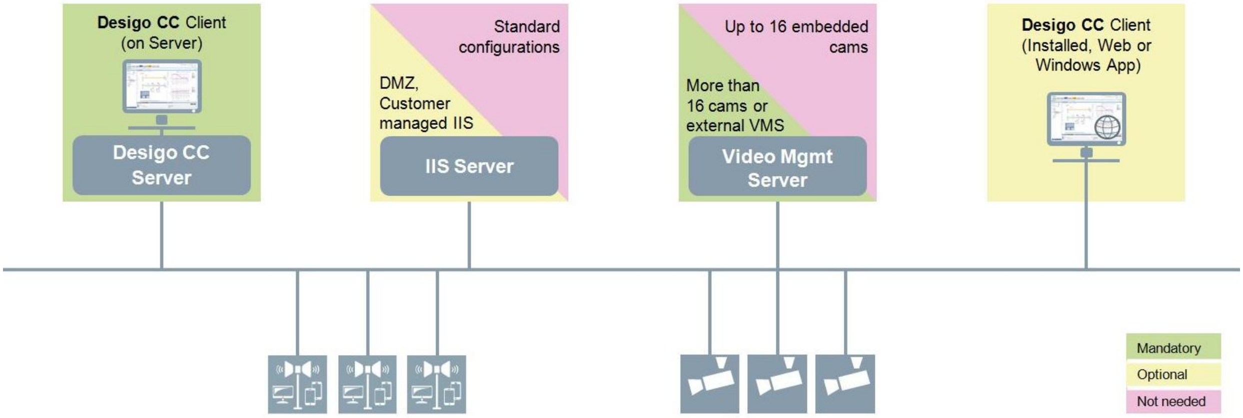
| PC | Role | Specification | Comments |
|---|---|---|---|
| DCC Server | Mandatory, needed for:<br>· BAS integration<br>· MNS drivers<br>· (IIS Server) | PC HW Cat C | Single PC deployment possible<br>**Note**: up to 5 MNS drivers and up to 5 BACnet drivers are supported |
| FEPs | Not needed | | |
| Clients | Optional additional client | PC HW Cat A | Total number of clients is limited to:<br>· 10 Installed Clients and<br>· 27 Windows App and Web Clients<br>That means:<br>· Up to 9 additional Installed Clients<br>· Up to 27 additional Windows App or Web Clients |
| Mobile App Clients | Optional mobile app client | | Up to 10/100 mobile app clients (see section 4.12, Remarks) |
| Dedicated Video Server | Not needed | | |
| SiPass Server | Not needed | | |
| Dedicated IIS Server | Not needed for standard configurations | | |
| | Recommended for configurations with:<br>· DMZ<br>· Customer managed IIS | PC HW Cat A | |
| Dedicated SQL Server | Not needed | | |

## 4.7 MNS and Video

Configuration Description:

- Video with up to 1000 cameras
- MNS: Multiple notification recipients as e.g. SMS, Pager, IP Phones, E-mail, PC, LED signs, loudspeaker, Facebook …

Topology:



Required Hardware:

| PC | Role | Specification | Comments |
|---|---|---|---|
| DCC Server | Mandatory, needed for:<br>· MNS drivers<br>· Video driver<br>· Video Server (for up to 16 embedded cameras)<br>· (IIS Server) | PC HW Cat B | Single PC deployment possible<br>**Note:** up to 5 MNS drivers are supported |
| FEPs | Not needed | | |
| Clients | Optional additional client | PC HW Cat A | Total number of clients is limited to:<br>· 10 Installed Clients<br>· 27 Windows App or Web Clients<br>· 2 if embedded video on DCC server<br>· 20 if embedded video with Video Server<br>· 25 if external VMS<br>That means:<br>· Up to 9 additional Installed Clients<br>· Up to 24 additional Windows App or Web Clients<br>**Note:** up to 16 video streams per client |
| Mobile App Clients | Optional mobile app client | | Up to 10/100 mobile app clients (see section 4.12, Remarks) |
| Dedicated Video Server | Not needed for up to 16 embedded cams | | |
| | Mandatory, if >16 embedded cams or for external VMS | See Milestone/ Siveillance VMS | VMS software (embedded or external) has to be installed on this PC |
| SiPass Server | Not needed | | |
| Dedicated IIS Server | Not needed for standard configurations | | |
| | Recommended for configurations with:<br>· DMZ<br>· Customer managed IIS | PC HW Cat A | |
| Dedicated SQL Server | Not needed | | |

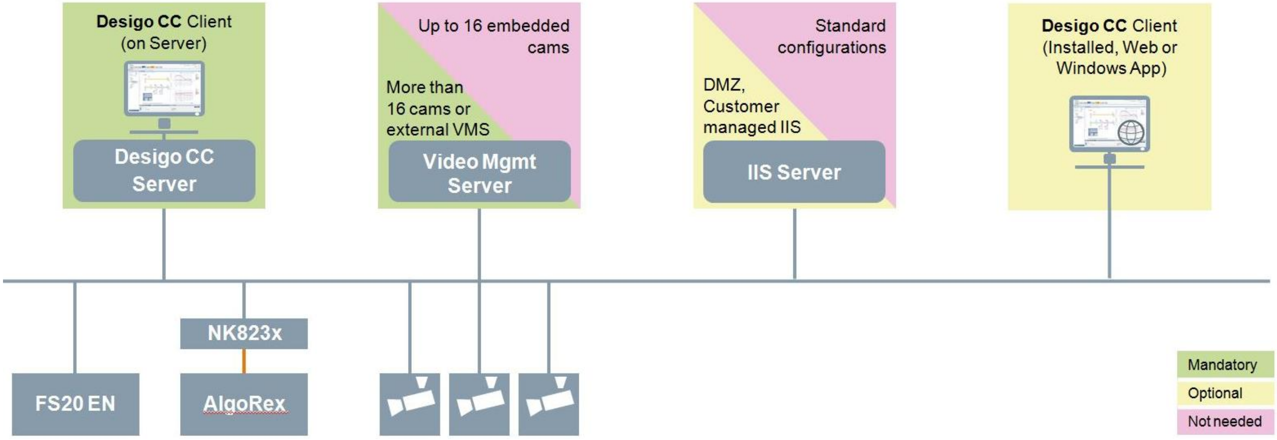
# 4.8 Fire and Video

Configuration Description:

- Fire System (FS20, AlgoRex and XLS/MXL)
- Up to 50,000 System objects for Fire (see dimensioning tool)
- Video with up to 1,000 (EN) / 128 (UL/ULC) cameras

## 4.8.1 EN Configurations

Topology:



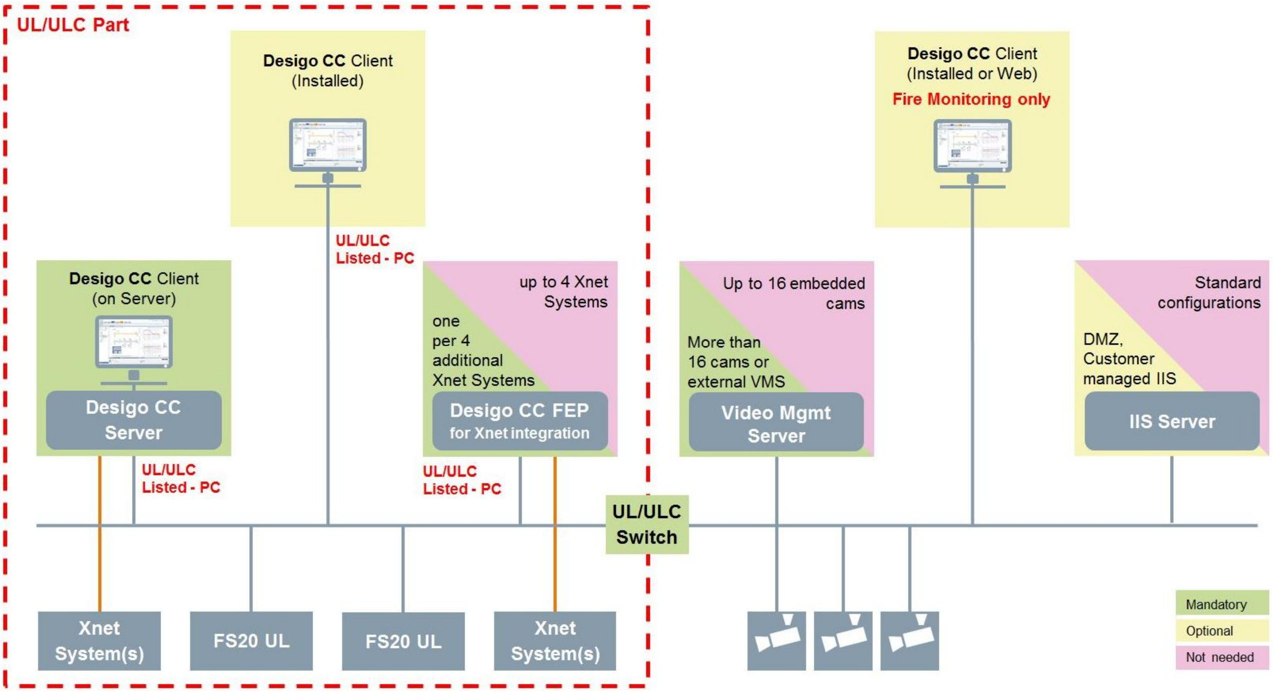
Required Hardware:

| PC | Role | Specification | Comments |
|---|---|---|---|
| DCC Server | Mandatory, needed for:<br>· Fire integration<br>· DCC Client<br>· Video driver<br>· Video Server (for up to 16 embedded cameras)<br>· (IIS Server) | PC HW Cat C | FS20: Up to 64 nodes per driver (see section 4.12, Remarks)<br>AlgoRex: Up to 4 C-Bus networks per driver (via NK823x)<br>Video: If >16 cameras: Video Server requires dedicated PC (see below).<br>Up to 16 video streams on client.<br>Server: Up to 5 drivers in total |
| FEPs | Not needed | | |
| Clients | Optional additional client for:<br>· Video Operation<br>· Fire Control | PC HW Cat A | Total number of clients is limited to:<br>· 10 Installed Clients<br>· 27 Windows App or Web Clients<br>· 2 if embedded video on DCC server<br>· 20 if embedded video with Video Server<br>· 25 if external VMS<br>That means:<br>· Up to 9 additional Installed Clients<br>· Up to 24 additional Windows App or Web Clients<br>**Note:** up to 16 video streams per client |
| Mobile App Clients | Optional mobile app client for:<br>· BAS operation<br>· Fire Control | | Up to 10/100 mobile app clients (see section 4.12, Remarks) |
| Dedicated Video Server | Not needed for up to 16 embedded cams | | |
| | Mandatory, if >16 embedded cams or for external VMS | See Milestone/ Siveillance VMS | VMS software (embedded or external) has to be installed on this PC |

| PC | Role | Specification | Comments |
|---|---|---|---|
| SiPass Server | Not needed | | |
| Dedicated IIS Server | Not needed for standard configurations | | |
| | Recommended for configurations with:<br>· DMZ<br>· Customer managed IIS | PC HW Cat A | |
| Dedicated SQL Server | Not needed | | |
| Misc | Ethernet Gateway for AlgoRex | NK823x | Up to 4 C-Bus networks per NK823x |

## 4.8.2 UL/ULC Configurations

Topology:



Remarks

- In case the distance between DCC stations and fire panels within the UL/ULC part is less than 20ft, copper wires in conduit can be used; otherwise fiber optics with listed switches are required.
- A total of 2 clients is supported if the Video server runs on the Desigo CC Server.
- A total of 20 clients is supported for embedded Video with dedicated Video Server
- Video restriction for UL/ULC: up to 16 streams per client
  - 4x4 layout: 16 streams at max. CIF resolution (352x288) / 10FPS
  - 1+7 layout: 1 stream 4CIF(704x576) / 25FPS and 7 streams 2CIF (704x288) / 25FPS
  - 2x2 layout: 4 streams at max. 4CIF resolution (704x576) / 25FPS
  - 1 layout: 1 FullHD (1920x1080) / 30FPS

Required Hardware:

| PC | Role | Specification | Comments |
|---|---|---|---|
| DCC Server | Mandatory, needed for:<br>· Fire integration (via DMS/NCC-2F and/or BACnet)<br>· DCC Client<br>· Video driver<br>· Video Server (for up to 16 embedded cameras)<br>· (IIS Server) | UL/ULC Listed - PC HW Cat C | XNET: Up to 4 XNET can be integrated. In case of more XNETs additional FEP's are required (see below)<br>FS20: Up to 64 nodes per driver (see section 4.12, Remarks)<br>Video: If >16 cameras: Video Server requires dedicated PC (see below).<br>Up to 16 video streams on client (with restrictions on video format)<br>Server: Up to 5 drivers in total |
| FEPs | Required for additional XNET connection via DMS/NCC-2F | UL/ULC Listed - PC HW Cat B | One additional FEP per 4 additional XNET connections is required<br>Up to 5 FEP's are supported. |
| | Not needed for up to 1 XNET | | |
| Clients (UL/ULC) | Optional additional client for:<br>· Fire Control<br>· Video operation | UL/ULC Listed - PC HW Cat A | Total number of clients (UL/ULC and non UL/ULC) is limited to:<br>· 7 Installed Clients<br>· 20 Web Clients<br>· 2 if emb video on DCC server<br>· 20 if emb video with Video Server<br>· 20 if external VMS<br>That means:<br>· Up to 6 additional Installed Clients<br>· Web Clients not allowed for fire control<br>**Note:** up to 16 video streams on client (with restrictions on video format)<br>Client could also be installed on FEP for XNET integration |
| Clients (non UL/ULC) | Optional additional client for:<br>· Fire Monitoring (no Control)<br>· Video operation | PC HW Cat A | Total number of clients (UL/ULC and non UL/ULC) is limited to:<br>· 7 Installed Clients<br>· 20 Web Clients<br>· 2 if emb video on DCC server<br>· 20 if emb video with Video Server<br>· 20 if external VMS<br>That means:<br>· Up to 6 additional Installed Clients<br>· Up to 19 additional Web Clients (no Windows App Clients)<br>**Note:** up to 16 video streams on client (with restrictions on video format) |
| Mobile App Clients | Optional mobile app client for<br>· Fire Monitoring (no Control)<br>· BAS operation | | Up to 10 mobile app clients (see section 4.12, Remarks) |
| Dedicated Video Server | Not needed for up to 16 embedded cams | | |
| | Mandatory, if >16 embedded cams or for external VMS | See Milestone/ Siveillance VMS | VMS software (embedded or external) has to be installed on this PC |
| SiPass Server | Not needed | | |
| Dedicated IIS Server | Not needed for standard configurations | | |
| | Recommended for configurations with:<br>· DMZ<br>· Customer managed IIS<br>· UL/ULC compliance | PC HW Cat A | |
| Dedicated SQL Server | Not needed | | |
| Misc. | UL/ULC switches | | |

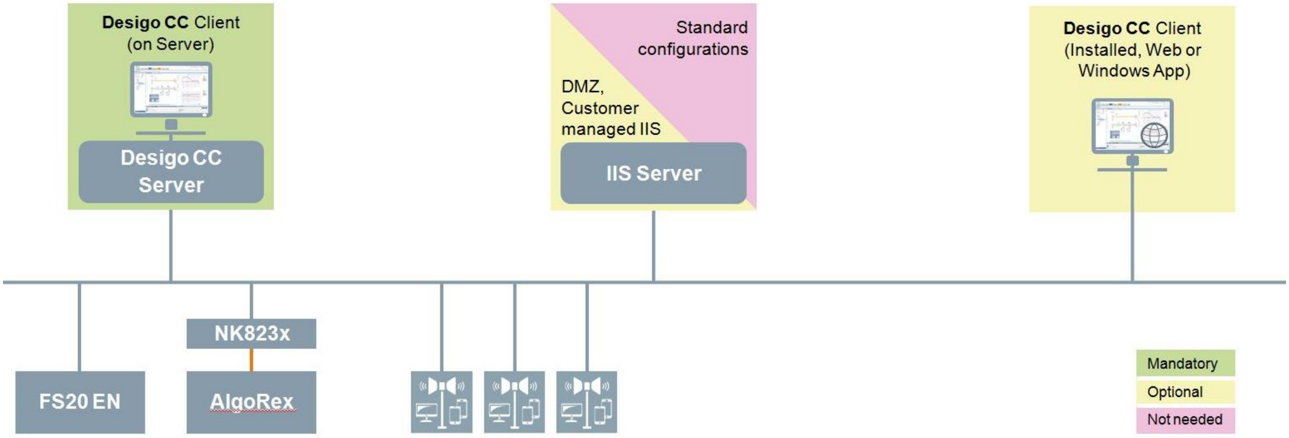
# 4.9 Fire and MNS

Configuration Description:

- Fire System (FS20, AlgoRex and XLS/MXL)
- Up to 50,000 System objects for Fire (see dimensioning tool)
- MNS: E-Mail notifications (UL/ULC) or multiple notification recipients as e.g. SMS, Pager, IP Phones, E-mail, PC, LED signs, loudspeaker, Facebook …(EN)

## 4.9.1 EN Configurations

Topology:

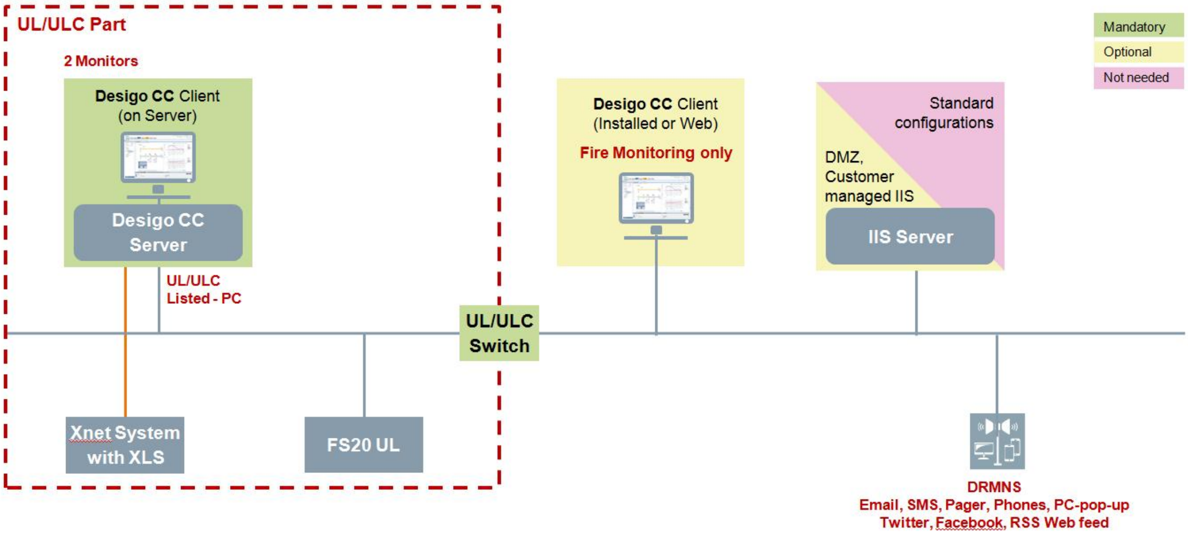

Desigo CC Client (on Server)
Desigo CC Server
Standard configurations
DMZ, Customer managed IIS
IIS Server
Desigo CC Client (Installed, Web or Windows App)
NK823x
FS20 EN
AlgoRex
Mandatory
Optional
Not needed

Required Hardware:

| PC | Role | Specification | Comments |
|---|---|---|---|
| DCC Server | Mandatory, needed for:<br>· Fire integration<br>· DCC Client<br>· MNS drivers<br>· (IIS Server) | PC HW Cat C | FS20: Up to 64 nodes per driver (see section 4.12, Remarks)<br>AlgoRex: Up to 4 C-Bus networks per driver (via NK823x)<br>**Note:** up to 5 MNS drivers and up to 5 BACnet drivers are supported |
| FEPs | Not needed | | |
| Clients | Optional additional client for:<br>· Fire Control<br>· MNS operation | PC HW Cat A | Total number of clients is limited to:<br>· 10 Installed Clients and<br>· 27 Windows App and Web Clients<br>That means:<br>· Up to 9 additional Installed Clients<br>· Up to 27 additional Windows App or Web Clients |
| Mobile App Clients | Optional mobile app client for:<br>· Fire Control | | Up to 10/100 mobile app clients (see section 4.12, Remarks) |
| Video Server | Not needed | | |
| SiPass Server | Not needed | | |
| Dedicated IIS Server | Not needed for standard configurations | | |
| | Recommended for configurations with:<br>· DMZ<br>· Customer managed IIS | PC HW Cat A | |
| Dedicated SQL Server | Not needed | | |
| Misc. | Ethernet Gateway for AlgoRex | NK823x | Up to 4 C-Bus networks per NK823x |

## 4.9.2 UL/ULC Configurations

Topology:

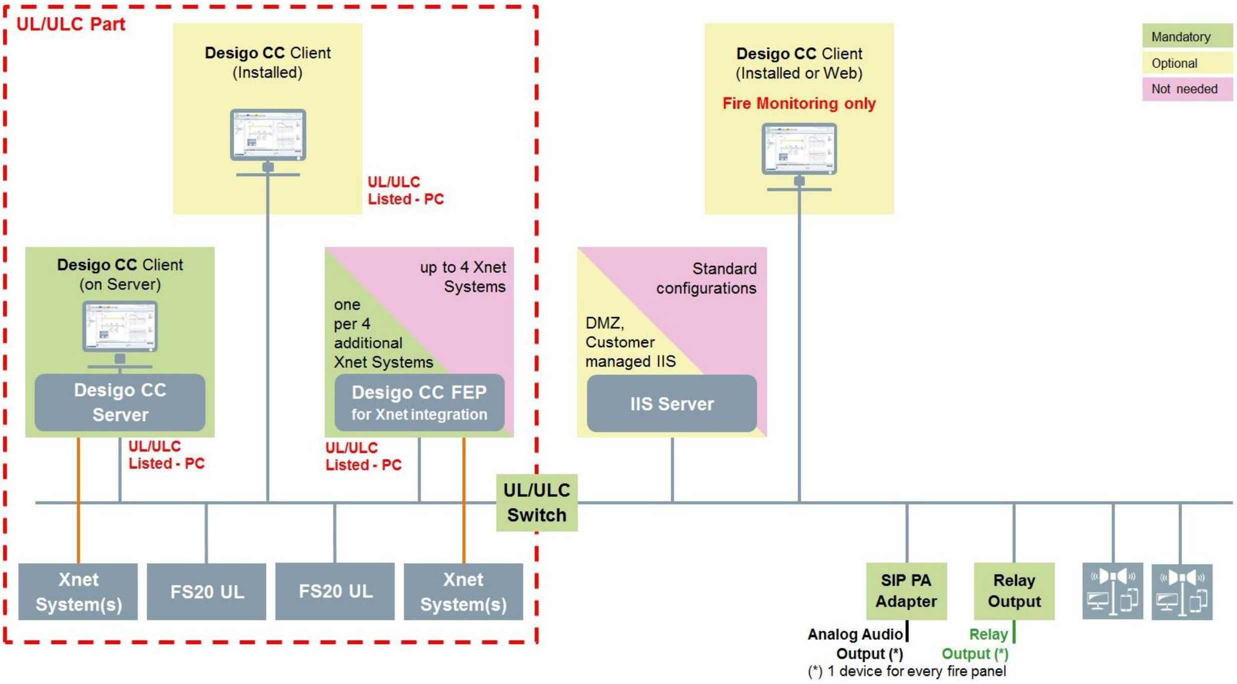


Required Hardware:

| PC | Role | Specification | Comments |
|---|---|---|---|
| DCC Server | Mandatory, needed for:<br>· Fire integration (via DMS/NCC-2F)<br>· DCC Client (with 2 monitors to separate GMS and MNS applications)<br>· MNS driver (for Email notifications only) | UL/ULC Listed - PC HW Cat C | XNET: Up to 4 XNET can be integrated. In case of more XNETs additional FEP's are required (see below)<br>FS20: Up to 64 nodes per driver (see section 4.12, Remarks)<br>MNS: Email notifications via UL2572 certified DRMNS Email server only. |
| FEP 1 to 5 | Required for additional XNET connection via NCC-2F | UL/ULC Listed - PC HW Cat B | One additional FEP per 4 additional XNET connections is required<br>Up to 5 FEPs are supported in total |
| | Not needed for up to 4 XNET | | |
| FEP 1 to 5 | Required for:<br>· FC20 integration via BACnet | UL/ULC Listed - PC HW Cat B | Up to 5 FEPs are supported in total |
| | Not needed without FS20 integration | | |
| Clients (UL/ULC) | Not needed | | Not supported by topology |
| Clients (non UL/ULC) | Not needed | | Not supported by topology |
| Mobile App Clients | Not needed | | Not supported by topology |
| Video Server | Not needed | | |
| SiPass Server | Not needed | | |
| IIS Server | Not needed | | |
| SQL Server | Not needed | | |
| Misc. | · XLS panel as ACU (in case of Xnet)<br>· UL/ULC switches | | |

## 4.9.3 UL/ULC Fire Part without MNS UL/ULC (Multiple Notification Channels)

Topology:



Required Hardware:

| PC | Role | Specification | Comments |
|---|---|---|---|
| DCC Server | Mandatory, needed for:<br>· Fire integration (viaDMS/ NCC-2F and/or BACnet)<br>· DCC Client<br>· (IIS Server) | UL/ULC Listed - PC HW Cat C | XNET: Up to 4 XNET can be integrated. In case of more XNETs additional FEP's are required (see below)<br>FS20: Up to 64 nodes per driver (see section 4.12, Remarks)<br>Server: Up to 5 drivers in total |
| FEP 1 to 5 | Required for additional XNET connection via DMS/NCC-2F | UL/ULC Listed - PC HW Cat B | One additional FEP per 4 additional XNET connections is required<br>Up to 5 FEPs are supported. |
| | Not needed for up to 4 XNET | | |
| MNS Server | Mandatory, needed for:<br>· MNS drivers<br>· DCC Client for MNS operation | PC HW Cat A, B or C (see MNS system descr.) | Up to 5 MNS drivers |
| Clients (UL/ULC) | Optional additional client for:<br>· Fire Control | UL/ULC Listed - PC HW Cat A | Total number of clients (UL/ULC and non UL/ULC) is limited to:<br>· 7 Installed Clients<br>· 20 Web Clients (Windows App Client not allowed)<br>That means:<br>· Up to 5 additional Installed Clients<br>· Web Clients not allowed for fire control<br>Client could also be installed on FEP for XNET integration |
| Clients (non UL/ULC) | Optional additional client for:<br>· Fire Monitoring (no Control) | PC HW Cat A | Total number of clients (UL/ULC and non UL/ULC) is limited to:<br>· 7 Installed Clients<br>· 20 Web Clients<br>That means:<br>· Up to 5 additional Installed Clients<br>· Up to 20 Web Clients (Windows App Client not allowed) |

| PC | Role | Specification | Comments |
|---|---|---|---|
| Mobile App Clients | Optional mobile app client for<br>· Fire Monitoring (no Control) | | Up to 10 mobile app clients (see section 4.12, Remarks) |
| Dedicated Video Server | Not needed | | |
| SiPass Server | Not needed | | |
| Dedicated IIS Server | Not needed for standard configurations | | |
| | Recommended for configurations with:<br>· DMZ<br>· Customer managed IIS<br>· UL/ULC Compliance | PC HW Cat A | |
| Dedicated SQL Server | Not needed | | |
| Misc. | · UL/ULC switches | | |

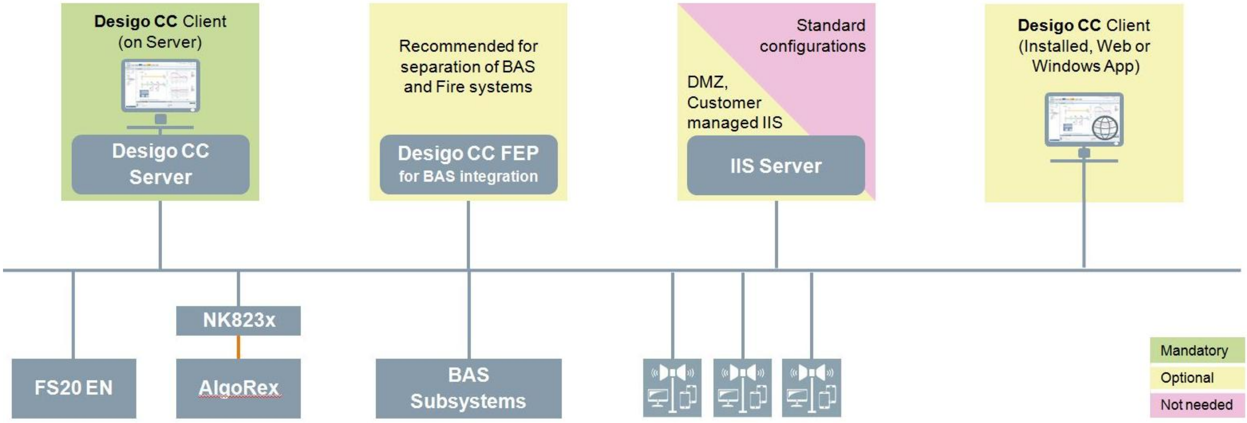
# 4.10 BAS, Fire and MNS

Configuration Description:

- Building Automation System (BAS)
- Fire System (FS20, AlgoRex and XLS/MXL)
- Up to 60,000 System objects for BAS and Fire (see dimensioning tool)
- MNS: E-Mail notifications (UL/ULC) or multiple notification recipients as e.g. SMS, Pager, IP Phones, E-mail, PC, LED signs, loudspeaker, Facebook …(EN)

## 4.10.1 EN Configurations

Topology:

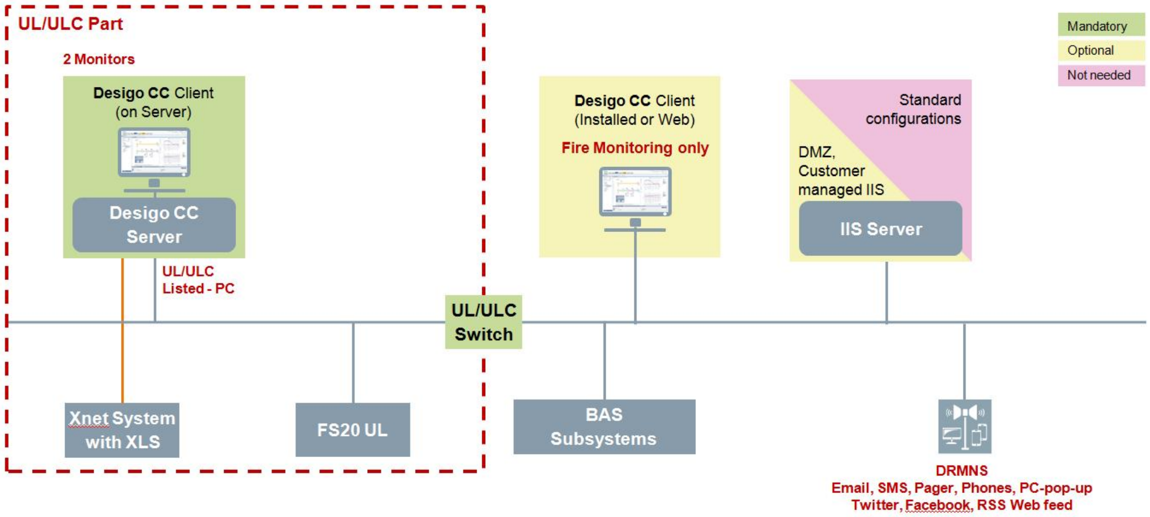

Desigo CC Client (on Server)
Desigo CC Server
Recommended for separation of BAS and Fire systems
Desigo CC FEP for BAS integration
Standard configurations
DMZ, Customer managed IIS
IIS Server
Desigo CC Client (Installed, Web or Windows App)
NK823x
FS20 EN
AlgoRex
BAS Subsystems
Mandatory
Optional
Not needed

Required Hardware:

| PC | Role | Specification | Comments |
|---|---|---|---|
| DCC Server | Mandatory, needed for:<br>· Fire integration<br>· (BAS integration)<br>· DCC Client<br>· MNS drivers<br>· (IIS Server) | PC HW Cat C | FS20: Up to 64 nodes per driver (see section 4.12, Remarks)<br>AlgoRex: Up to 4 C-Bus networks per driver (via NK823x)<br>**Note:** up to 5 MNS drivers and up to 5 BACnet drivers are supported |
| FEP 1 | Optional for BAS integration | PC HW Cat B | Dedicated FEP is recommended to separate the BAS from the Fire system.<br>**Note:** online/auto configuration not supported on FEP. |
| FEP 2 to 5 | Not needed | | |
| Clients | Optional additional client for:<br>· Fire Control<br>· BAS & MNS operation | PC HW Cat A | Total number of clients is limited to:<br>· 10 Installed Clients and<br>· 27 Windows App and Web Clients<br>That means:<br>· Up to 9 additional Installed Clients<br>· Up to 27 additional Windows App or Web Clients<br>Clients could also be installed on FEPs |
| Mobile App Clients | Optional mobile app client for<br>· Fire Monitoring (no Control) | | Up to 10/100 mobile app clients (see section 4.12, Remarks) |
| Video Server | Not needed | | |
| SiPass Server | Not needed | | |
| Dedicated IIS Server | Not needed for standard configurations | | |
| | Recommended for configurations with:<br>· DMZ | PC HW Cat A | |

| PC | Role | Specification | Comments |
|---|---|---|---|
| | · Customer managed IIS | | |
| Dedicated SQL Server | Not needed | | |
| Misc. | Ethernet Gateway for AlgoRex | NK823x | Up to 4 C-Bus networks per NK823x |

## 4.10.2 UL/ULC Configurations



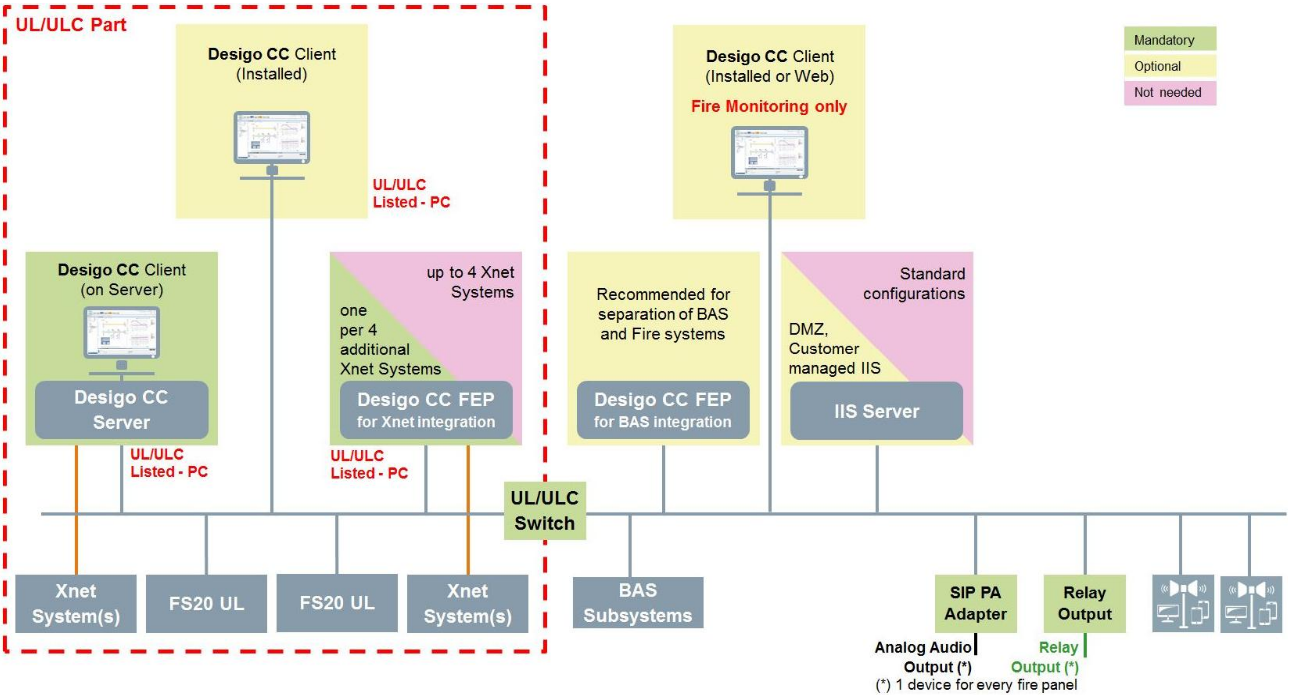
Topology:

Required Hardware:

| PC | Role | Specification | Comments |
|---|---|---|---|
| DCC Server | Mandatory, needed for:<br>· Fire integration (via NCC-2F)<br>· DCC Client (with 2 monitors to separate GMS and MNS applications)<br>· MNS driver (for Email notifications only) | UL/ULC Listed - PC HW Cat C | XNET: Up to 4 XNET can be integrated. In case of multiple XNETs additional FEP's are required (see below)<br>FS20: Up to 64 nodes per driver (see section 4.12, Remarks)<br>MNS: Distributed Recipients MNS (DRMNS) U2572 approved. |
| FEP 1 to 5 | Required for additional XNET connection via DMS/NCC-2F | UL/ULC Listed - PC HW Cat B | One additional FEP per 4 additional XNET connections is required<br>Up to 5 FEPs are supported in total |
| | Not needed for up to 4 XNET | | |
| FEP 1 to 5 | Required for:<br>· FC20 integration via BACnet<br>· BAS integration via BACnet | UL/ULC Listed - PC HW Cat B | Up to 5 FEPs are supported in total |
| Clients (UL/ULC) | Not needed | | Not supported by topology |
| Clients (non UL/ULC) | Not needed | | Not supported by topology |
| Mobile App Clients | Not needed | | Not supported by topology |
| Video Server | Not needed | | |
| SiPass Server | Not needed | | |
| IIS Server | Not needed | | |
| SQL Server | Not needed | | |
| Misc. | · XLS panel as ACU (in case of Xnet)<br>· UL/ULC switches | | |

### 4.10.3 UL/ULC Fire Part without MNS UL/ULC (Multiple Notification Channels)

Topology:



Required Hardware:

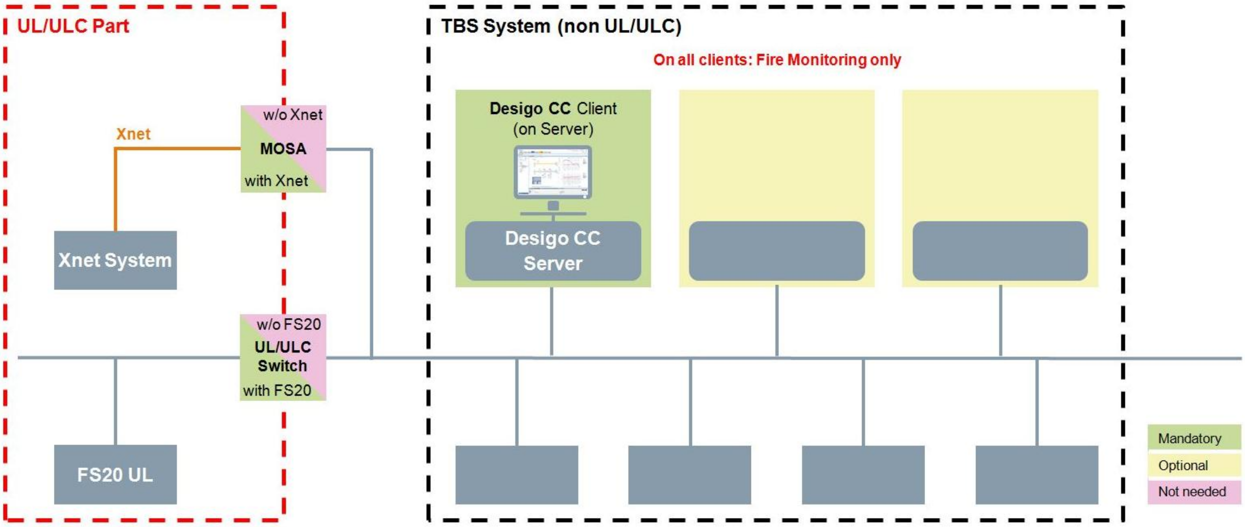
| PC | Role | Specification | Comments |
|---|---|---|---|
| DCC Server | Mandatory, needed for:<br>· Fire integration (via DMS/NCC-2F and/or BACnet)<br>· DCC Client<br>· (IIS Server) | UL/ULC Listed - PC HW Cat C | XNET: Up to 4 XNET can be integrated. In case of multiple XNETs additional FEP's are required (see below)<br>FS20: Up to 64 nodes per driver (see section 4.12, Remarks)<br>Server: Up to 5 drivers in total |
| FEP 1 | Optional for BAS integration | PC HW Cat B | Dedicated FEP is recommended to separate the BAS from the Fire system.<br>**Note:** online/auto configuration not supported on FEP. |
| FEP 2 to 5 | Required for additional XNET connection via DMS/NCC-2F | UL/ULC Listed - PC HW Cat B | One additional FEP per 4 additional XNET connections is required.<br>Up to 4 FEPs for XNET are supported. |
| | Not needed for up to 4 XNET | | |
| MNS Server | Mandatory, needed for:<br>· MNS drivers<br>· DCC Client | PC HW Cat A, B or C (see MNS system descr.) | Up to 5 MNS drivers |
| Clients (UL/ULC) | Optional additional client for:<br>· Fire Control<br>· BAS operation | UL/ULC Listed - PC HW Cat A | Total number of clients (UL/ULC and non UL/ULC) is limited to:<br>· 7 Installed Clients<br>· 20 Web Clients (Windows App Client not allowed)<br>That means:<br>· Up to 5 additional Installed Clients<br>· Web Clients not allowed for fire control<br>Client could also be installed on FEP for XNET integration |
| Clients (non UL/ULC) | Optional additional client for:<br>· Fire Monitoring (no Control)<br>· BAS operation | PC HW Cat A | Total number of clients (UL/ULC and non UL/ULC) is limited to:<br>· 7 Installed Clients<br>· 20 Web Clients (Windows App Client not allowed)<br>That means:<br>· Up to 5 additional Installed Clients<br>· Up to 20 Web Clients<br>Client could also be installed on FEP for BAS integration |
| Mobile App Clients | Optional mobile app client for<br>· Fire Monitoring (no Control) | | Up to 10 mobile app clients (see section 4.12, Remarks) |
| Dedicated Video Server | Not needed | | |
| SiPass Server | Not needed | | |
| Dedicated IIS Server | Not needed for standard configurations | | |
| | Recommended for configurations with:<br>· DMZ<br>· Customer managed IIS<br>· UL/ULC Compliance | PC HW Cat A | |
| Dedicated SQL Server | Not needed | | |
| Misc. | · UL/ULC switches | | |

# 4.11 Fire Monitoring-Only without UL/ULC Server Hardware

Configuration Description:

- Any non UL/ULC TBS system with Desigo CC management platform
- UL/ULC Fire detection system

Topology:



Required Hardware:

| PCs | Role | Specification | Comments |
|---|---|---|---|
| DCC Server | Mandatory, needed for:<br>· Integration of all TBS subsystems<br>· DCC Client | See dimensioning tool | Note: Fire Monitoring-Only. No control. |
| FEPs | Optional | | |
| Clients | Optional additional client | | Note: Fire Monitoring-Only. No control. |
| Mobile App Clients | Optional mobile app client | | Note: Fire Monitoring-Only. No control. |
| Video Server<br>SiPass Server<br>IIS Server<br>SQL Server | Optional, depending on TBS system | | |
| MOSA Monitoring-Only Solution Assembly | Not needed without Xnet | | |
| | Mandatory for Xnet integrations | | Available from Siemens BT<br>Part Number: S54465-C62-A1 |
| UL/ULC Switch | Not needed without FS20 UL | | |
| | Mandatory for FS20 UL integrations | | |

## 4.12 Remarks to Configurations

General:

- Please always check the dimensioning tool for HW recommendations based on the exact number of connected subsystems and detectors

Limitations for FS20 Integrations:

- Up to 64 FS20 nodes (panels) are possible per Desigo CC BACnet driver.
- Stand-alone FS20 and networked FS20 nodes are supported.
- One FS20 EN system can have up to 4 SAFEDLINK networks with up to 16 panels.
- One FS20 UL network can have up to 32 (FV-Net or Ethernet communication) or up to 16 (SAFEDLINK) nodes.
- Desigo CC BACnet driver supports 4 networks as long as 64 FS20 node limit is not exceeded.

Number of Clients:

- Total number of installed clients is limited to 10.
- For UL/ULC compliant topologies, the total number of installed clients is limited to 7.
- These figures include the client on the server, the clients within UL/ULC part and clients outside the UL/ULC part.

SQL Server:

- Please check the dimensioning tool for MS/SQL version required.
- A dedicated PC for the SQL server is recommended if fill level on DCC server is above 70%.

Web Services:

- Mobile App clients and web service sessions for north-bound connectivity need one Web service session each. The total number of active Web service sessions is limited to:
  - 10, if IIS runs on Windows 7/8.1
  - 100, if IIS runs on Windows Server 2008 R2/2012 R2
- For UL/ULC topologies the total number of Mobile App clients is limited to 10.

Issued by
Siemens Switzerland Ltd
Building Technologies Division
International Headquarters
Gubelstrasse 22
CH-6301 Zug
Tel. +41 41-724 24 24
www.siemens.com/buildingtechnologies

Document ID A6V10415500_en_a_30

Edition 2018-01-15