SIEMENS

Cerberus® LMSmodular Basic Module Ver. 2.4

Application Examples

Cerberus
Security
for People
and Assets

Siemens Building Technologies
Cerberus Division

Document changes in Version 2.4

Topic	Comments
Gateway	GW-20 and GW-21 replaced GW-00 and GW-01, respectively
Subsystems	CC-30 CerPass, MM/MF, Transliner and WSE 4100 NexSentry in native mode are now supported
Architectures	New examples
System parameters	Improved system capacity in most of the parameter limits

1 Introduction

LMSmodular is a management system for integrating security and safety systems. It allows central monitoring and control of security installations used in a variety of applications.
The LMSmodular system is presently installed in different versions in more that 1000 sites over the world.
Among the many benefits the user can get from adopting LMSmodular there are:

- the system flexibility - you can build the configuration best fitted to your actual plant. LMSmodular can be used for brand new installation as well as to improve the performances of existing system, integrating the already installed hardware.
- the software modularity - LMSmodular, as the name itself suggest, is composed by various modules. To start with, you buy just want you need, but you can upgrade the system when purchasing new modules as soon as your needs increase.
- a high reliability - LMSmodular is based on the concept of autonomous subsystems and distributed control. The decisions are taken at the lowest level possible and therefore actions are undertaken at the maximum speed. Moreover, a fault at higher levels do not affect the system capability to respond to events. To further reduce the risks associated to faults, redundant configurations can be implemented;
- the openness toward systems supplied by third parties. Using either the NISE00 or FHI Pads, or applying DDE solutions, the LMSmodular system can talk to systems designed and manufactured by others. You can therefore integrate into an LMSmodular plant technological devices or other security devices, provided that they comply with LMSmodular specifications.

1.1 For further information

You can refer to the following Cerberus documents to have information about specific products mentioned in this document. In these manuals you will find also information about how to install and/or configure software and hardware parts needed to properly set up your system.

- GW-21 Technical Manual e1481
- GW-20 Technical Manual e1478
- LMSmodular Installation Manual e1862
- LMSmodular User Manuale 1865
- LMSmodular Configuration Guide e1863
- LMSmodular Configuration Reference e1864
- NISE_CNF Configuration manual e1150
- FHI Pad Engineering Guidelines e1143
- IMS2000 Engineering Guidelines e1142
- CDDL Cerberus Dati Data Link
  - Data Link Protocol Description CDI-135-017-E
- CDSF Cerberus Dati Standard Format
  - Application Protocol Description CDI-130-017-E
- LMSmodular System description V2.4 e1867
- LMSmodular Software Product description V2.4 e1866

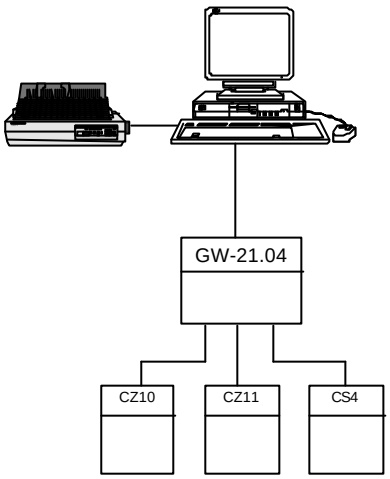
2 Network configuration examples

The following examples are intended to show some typical cases of network configuration.

2.1 Example 1: small system fire + intrusion

System composed by

- One operating station
- 1 CZ10
- 1 CS11
- 1 CS4

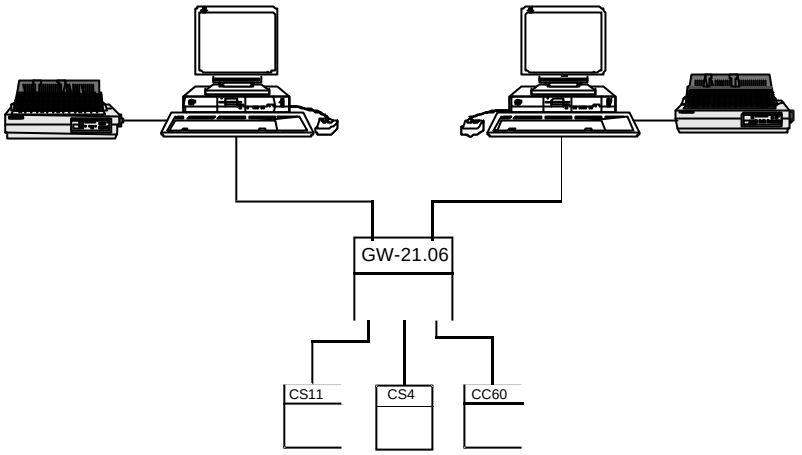


You can use

- one Gateway GW-21.04. This solution has the advantage to be a low cost, but you cannot expand the system. The GW-21.04 has only four lines and they are occupied by three subsystems and one operating station. No multistation configuration is possible.

2.2 Example 2: two stations monitoring fire + gas + intrusion

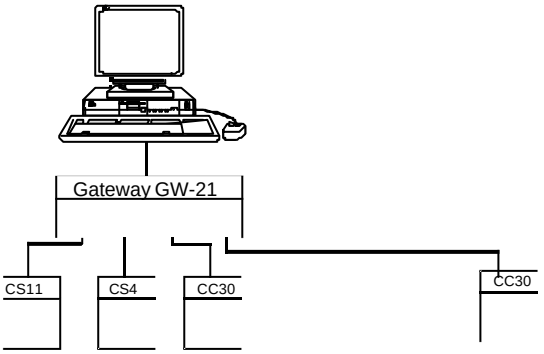
System composed by
- Two operating stations
- 1 CS11
- 1 CS4
- 1 CC60
- availability of one line for future expansion



You can use
- one Gateway GW-21.06. A low cost solution, with one line left to connect one more subsystem. However, you cannot add more operating stations. Two is the maximum number or operating stations supported by the GW-21.

2.3 Example 3: access control + intrusion +fire

System composed by
One operating station
1 CS11
1 CS4
2 CC30

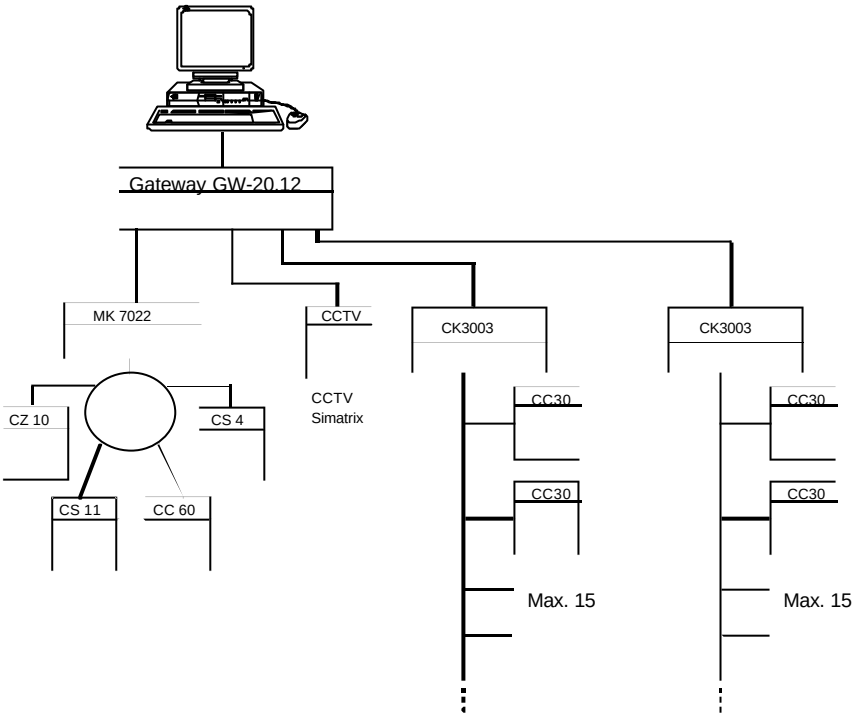


Note: Westinghouse AC units (422, 818, 4100, 4104) may also be connected.

2.4 Example 4: medium system fire + gas + intrusion + CCTV + access control

System composed by

- One operating station
- 1 Cerloop
- 1 CCTV Simatrix
- Some CC30 (max. 15 per line) connected in a multidrop configuration using a serial RS485 line.



A protocol converter, from RS485 to RS232 is needed. You cannot implement this system using a GW-21 although four lines are required. Due to EPROM firmware limits, you have to use

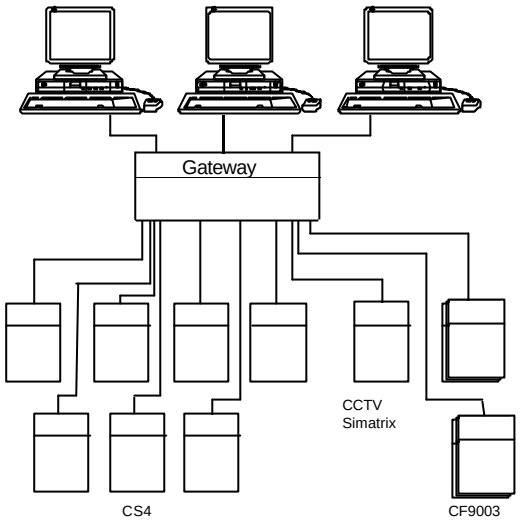
- one Gateway GW-20.12, equipped with one CMS Pad and three Subsystem Pads. In this case three Subsystem Pads are required because the Cerloop, CCTV and Cer-Pass firmware protocols cannot reside on the same EPROM. The system can be easily expanded at no cost to include other subsystems. 8 lines are still available to support for instance CS11 or CS4 in a point to point connection.

Note: Westinghouse AC units (422, 818, 4100, 4104) may also be connected.

2.5 Example 5: large system intrusion + CCTV

System composed by

- Three operating stations
- 7 CS4
- 1 CCTV
- 2 CF9003 clusters



The system must be implemented using a GW-20 because 10 lines are required. You have to use:

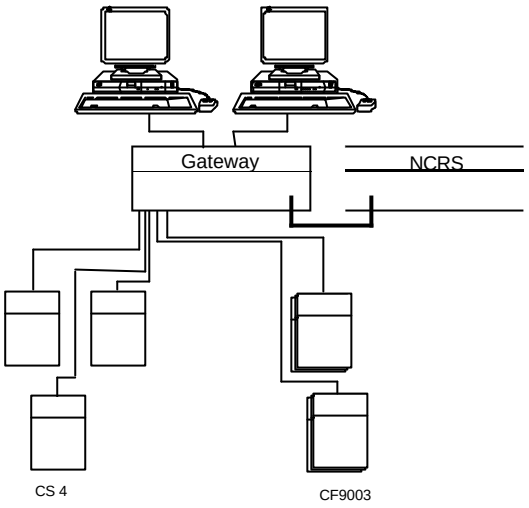
- one Gateway GW-20.12 equipped with one CMS Pad and three Subsystem Pads. To one Subsystem pad you can connect the 3 CS4 and the CCTV subsystems, on the second Subsystem Pad three CS4 and one line can be connected, while the CS4 and the line remaining can be linked to the third Subsystem Pad. Two lines are available to connect in a future implementation two subsystems and one more operating station can be added at no cost. Two slots are free to accommodate two other Subsystem Pads.

The lines are RS-485 bus with a IC-2 interface (see also example 9).

2.6 Example 6: IMS2000

System composed by

- Two operating stations
- 3 CS4
- integration with technological plant supervision system MS 2000 is required
- 2 CF9003 clusters



The system must be implemented using a GW-20 because the integration with technological plant is required. You have to use:

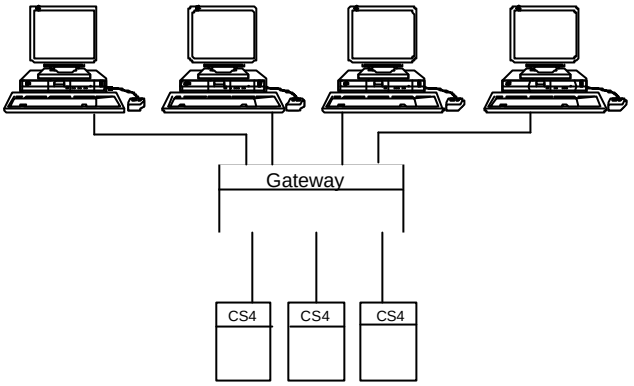
- one Gateway GW-20 equipped with one CMS Pad, two Subsystem Pads and one NISE00 Pad. To one Subsystem Pad you can connect the 2 CS4 and one line, and on the second Subsystem Pad one CS4 and one line can be connected. The NISE00 is used to connect the Gateway to the MS 2000. Three lines are available to connect in a future implementation three more subsystems without additional costs. Two more operating stations can be added at no cost. There are two slots available to accommodate two other Subsystem Pads. In its full expansion this gateway can have only 16 lines toward subsystems because the NISE00 Pad takes up one slot.

The same consideration applies if the connections should be performed toward a Foreign Supervision System using the FHI Pad.

2.7 Example 7: four stations monitoring intrusion

System composed by

- Four operating stations
- 3 CS4



The system must be implemented using a GW-20 to satisfy the requirement for four operating stations.

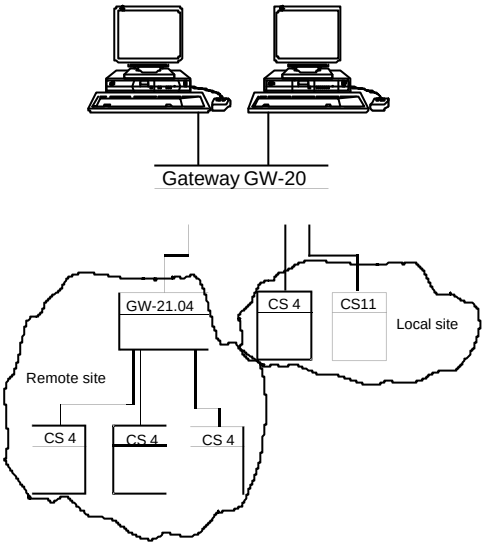
To implement the system you must use

- one Gateway GW-20.04 equipped with one CMS Pad and one Subsystem Pad. You can not connect more operating stations. You still have one line to add a further subsystem and four slots available to insert more Subsystems Pads.

2.8 Example 8: local + remote sites

System based on two level architecture composed by

- Two operating stations
- 4 CS4. Three of them are remote installed and connected to the secondary gateway, one to the concentrator
- 1 CS11
- one secondary gateway GW-21.04
- one concentrator Gateway GW-20



You have to use:

- one Gateway GW-20 equipped with one CMS Pad, one Subsystem Pad and one NetM Pad. To the Subsystem Pad are connected the local CS4 and CS11. The NetM Pad links the secondary Gateway using the CMSDL protocol. The three CS4 are connected to the GW-21.04.
  - There are:
    - two lines available for local subsystems to be connected to the existing Subsystem Pad
    - three lines available for secondary GW-21 to be connected to the existing NetM Pad
    - 3 slots free in the Gateway GW-20 to host other Pads

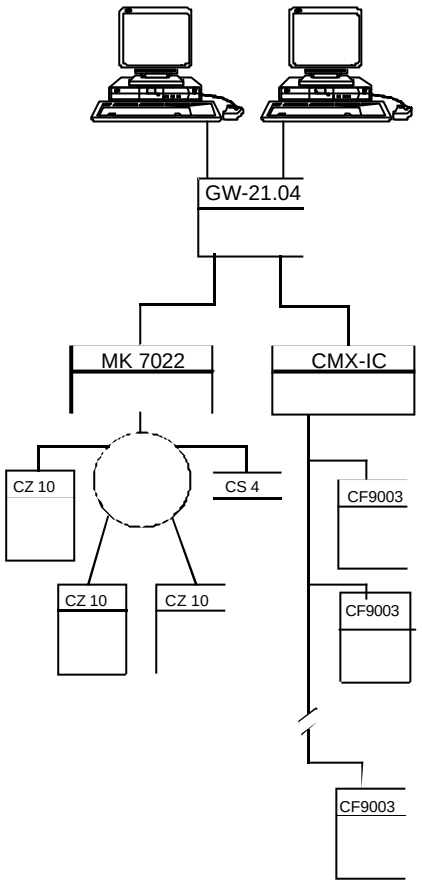
  GW21 may be expanded to a GW21-06, so that one more subsystem (e.g. CS4 or CS11) can be connected.

Also, a local LMS may then be also connected to the GW21.

2.9 Example 9: small system Cerloop + CF9003

System composed by:

- Two operating stations
- one Cerloop. One CS4 and three CZ10 (or CS11) are connected to the MK 7022
- a cluster of three CF9003 connected in multidrop to a single IC-2

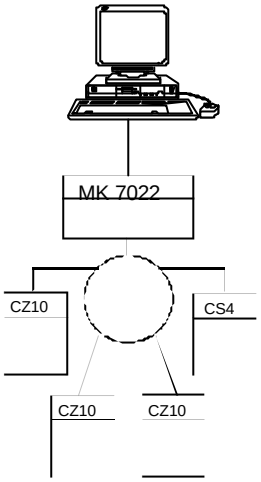


To implement the system you must use:

- a Gateway GW-21.04 that is fully saturated, i.e. no more lines are available to connect other device directly to it. However, you can connect more CZxx to the Cerloop or more CF9003 to the IC-2.

2.10 Example 10: small system Cerloop

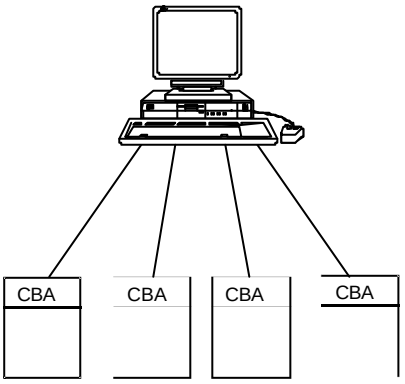
System composed by:
- One operating stations
- one Cerloop. One CS4 and three CZ10 (or CS11) are connected to the MK 7022



The system is implemented as a null network, i.e. the MK 7022 that controls the Cerloop is directly connected to the Operating station.

2.11 Example 11: CBA fire

System composed by:
- one operating station
- four CBA (CDDL / CDSF)

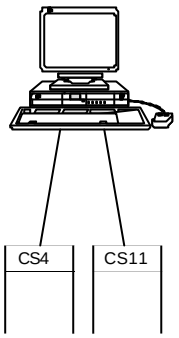


The system is implemented as a null network, i.e. the CBA is directly connected to the Operating station. Note, in order to support 4 serial lines (COM1:, COM2:, COM3:, COM4:), that special PC hardware is needed.

2.12 Example 12: very small system fire + intrusion

System composed by:

- one CS4
- one CS11

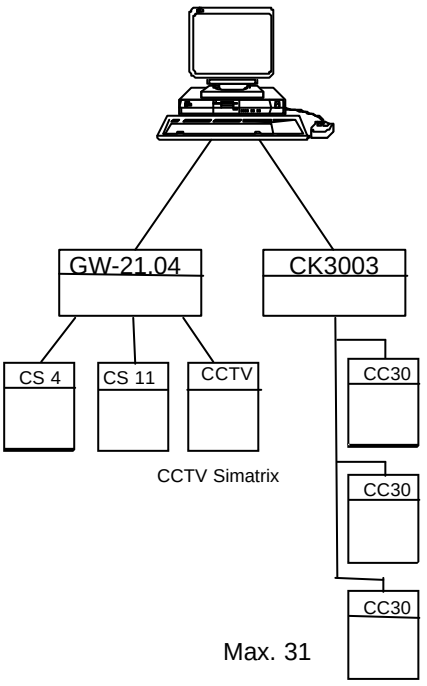


The system is implemented as a null network, i.e. the CS4 and the CS11 are directly connected to the Operating station.

2.13 Example 13: small system fire + intrusion + CCTV + access control

System composed by:

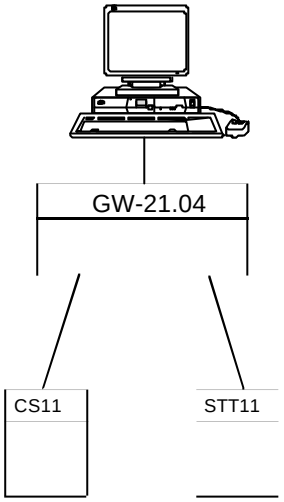
- one operating station
- one CS4
- one CS11
- one CCTV Simatrix
- three CC30



The station monitors fire, intrusion and CCTV via a GW-21.04 gateway and access control directly connected.

2.14 Example 14: small system fire (CS11 + STT11)

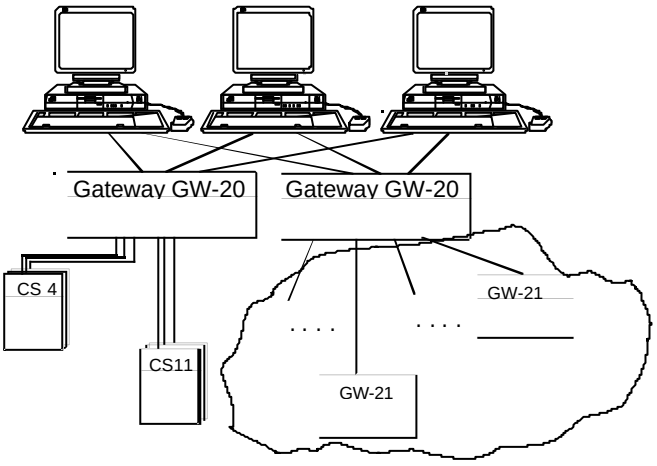
System composed by:
- one operating station
- one CS11
- one STT11



A GW-21.04 can be applied, one serial line of the gateway is still available for either a second station or an additional subsystem.

2.15 Example 15: large system with redundant stations

System composed by:
- three operating stations
- two GW20
- one local set of Csxx
- 20 remote sites with up to 4 Csxx

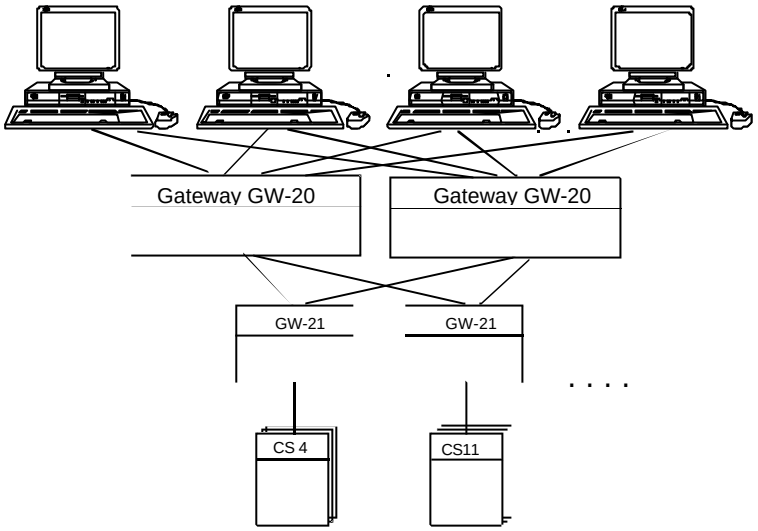


The system is partially a one level network (local control panels) and partially a two level network (remote control panels). The operating stations are in hot stand-by because they are cross connected to GW-20. Should one of them fail, the other will send messages anyway to the operating stations.

2.16 Example 16: large system with redundant network

System composed by:

- four operating stations cross connected to Gateways GW20
- two GW20 cross connected to Gateway GW21
- 24 GW21 connected to CS4 and CS11 control panels



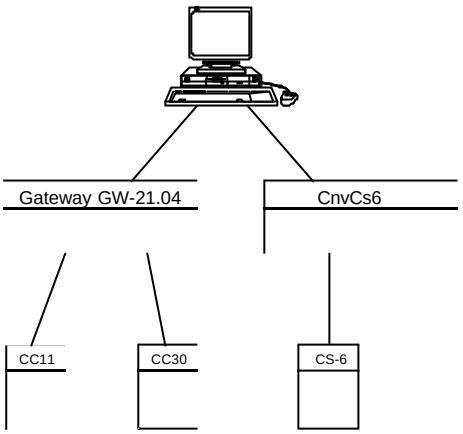
The system implements a network hot stand-by. Even in case of communication lines failures, the messages have an alternative path to reach the operating stations which are also hot stand-by.

The GW21 are necessary for duplicating the connections of the control units (usually are GW21 per unit).

2.17 Example 17: small system fire + access control + intrusion

System composed by:
- one operating station
- one CC11
- one CC30
- one CS6 (intrusion only)

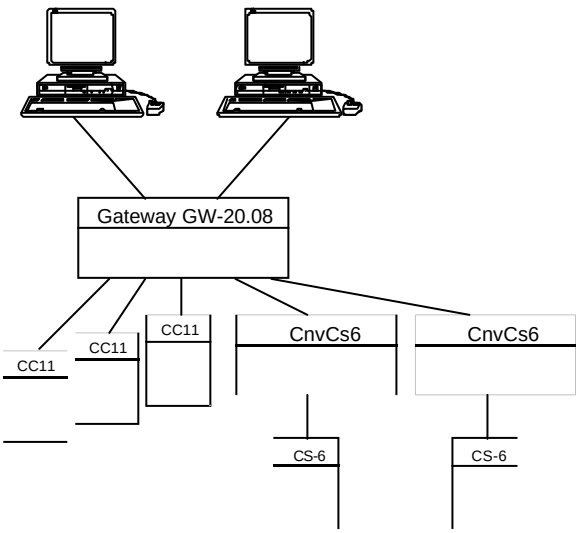
The station monitors fire and access control via a GW21-04 gateway; whereas Guarto control unit is connected to the station via a Cnv-CS6 converter.



2.18 Example 18: small system fire + intrusion/access control

System composed by:
- two operating station
- one CS11
- two CS6 (intrusion/access control)

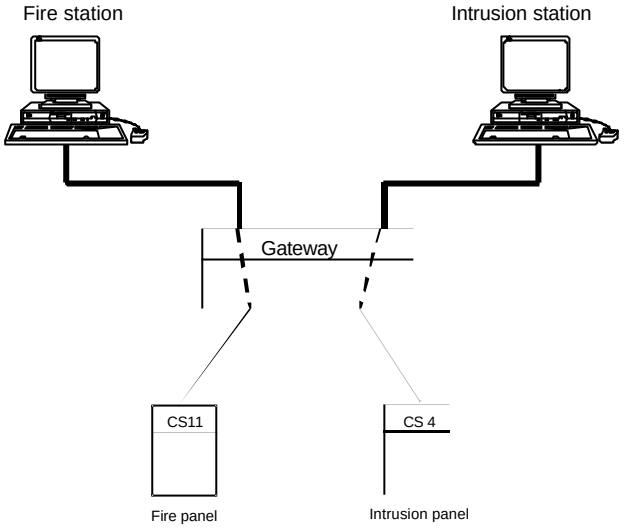
To implement the system you must use:
- a gateway 20-08 with a NetMPad board connected to the Guarto central units (CS6).



3 OS configuration examples

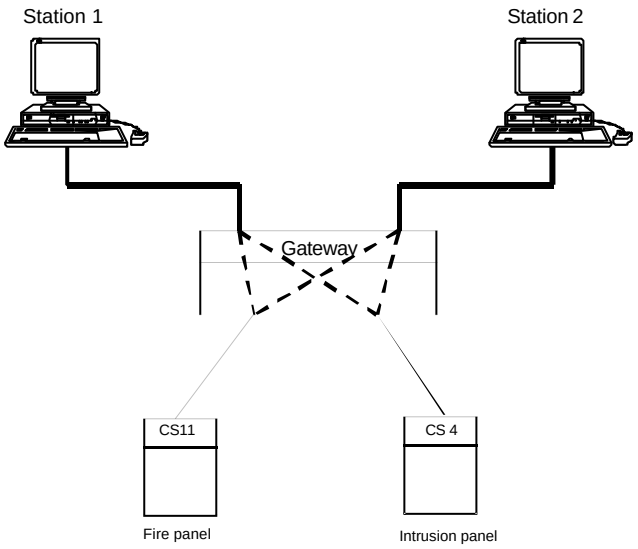
3.1 Example 1: fire station + intrusion station

The operating station can be specialized at Gateway level. The Gateway routes information from the subsystem only to the operating station it has been configured to.



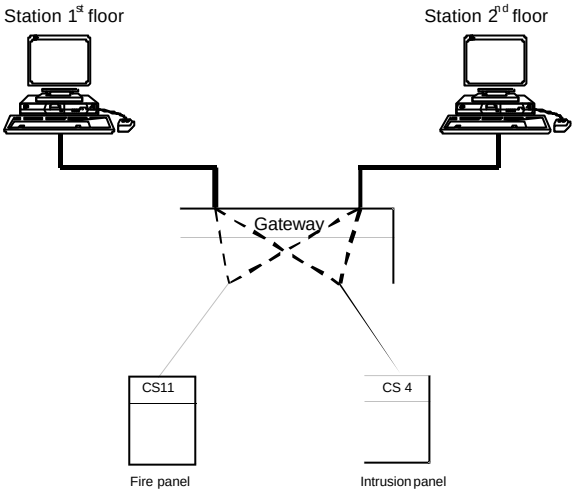
3.2 Example 2: two multi-discipline stations

In this example, the operating station are not specialized. The Gateway routes all information from the subsystem to any operating station connected to it.



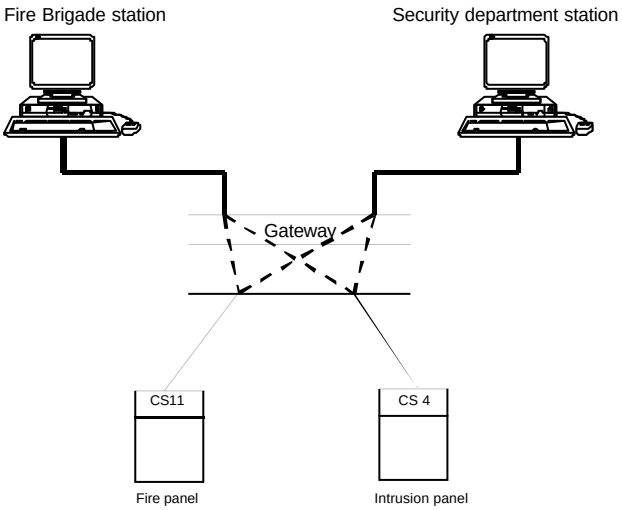
3.3 Example 3: stations specialized by site

This third example shows a configuration with operating stations that are specialized through software configuration. The Gateway routes all information from the subsystem to any operating station connected to it, but the operating station have different database. Therefore, the information displayed to the operators are different. This configuration allows the operating station differentiation on the basis of functions. One of them could be used to monitor a subset of the installed devices and the other another subset. Here "subset" means even the single detector or actuator, and no longer, as in Example 1, the control panels. You can for instance configure the operating station to display data about different building storeys by differentiating the configuration at sensor/actuator level.



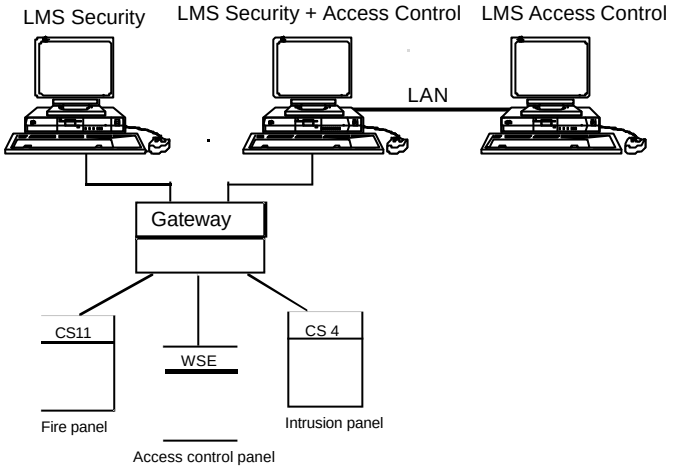
3.4 Example 4: station specialized by discipline

In this example two operating stations are configured. The first is installed at the fire brigade offices, the second in the security department. The plant includes both fire and security control panels that are configured on both the operating station. On the fire brigade station however a security alarm generates only an anomaly event, while a fire event triggers a severe alarm. On the contrary the security department sees as severe alarms all events generated by security control panels and as anomalies those generated by fire control panels.



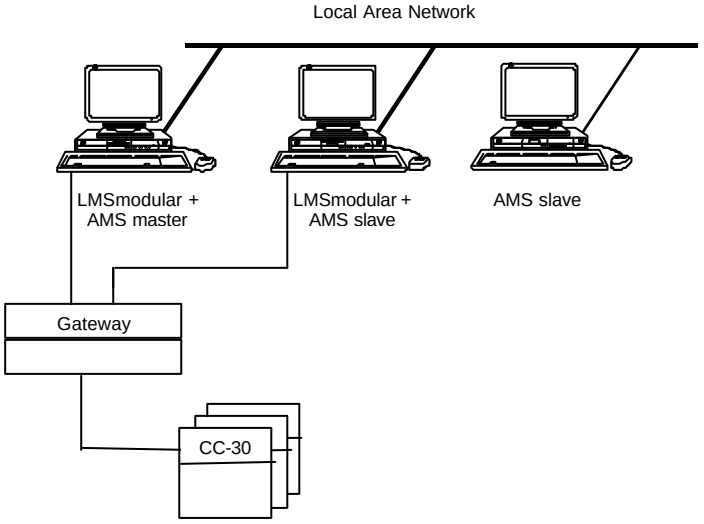
3.5 Example 5: access control stations

In this example a system that includes access control is presented. A total of three operating stations are installed; two of them are connected to a gateway that controls fire, intrusion and access control panels. A third station is connected via a local area network to another station.
The software installed on the three stations is different. In the first one the base LMSmodular allows for security monitoring. The next station is equipped with both base module and ACW package that allows for complete access control configuration. Finally, the third station (without direct GW connection) is dedicated to access control only. It can configure the data, but it cannot manage events.
ACW package supports Westinghouse unit 422, 818, 4100 and 4104.



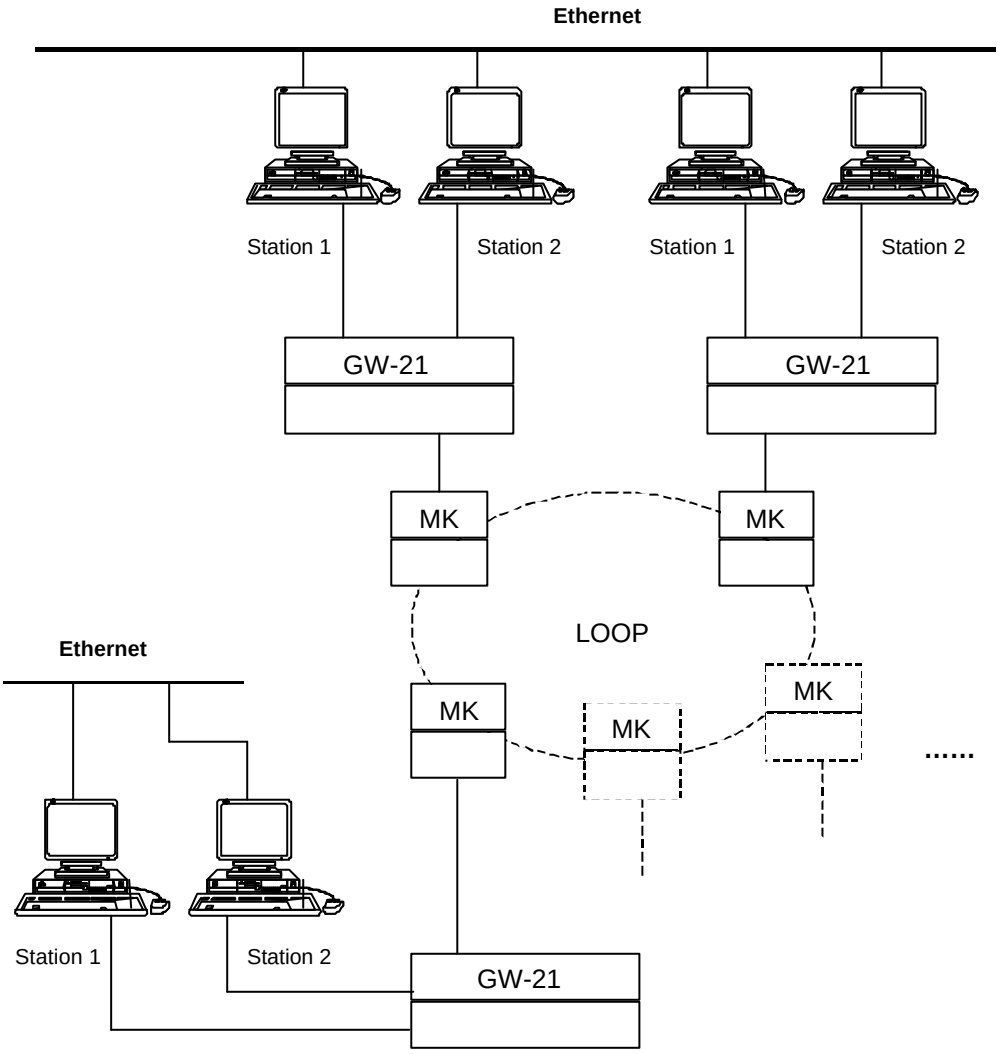
3.6 Example 6: LMS and CerPass AMS

LMSmodular stations may also run the CerPass AMS software for a combined Safety, Security, and Access Control monitoring solution. The AMS architectures foresee a *master* station that should be integrated with LMSmodular, and a number of *slave* stations, that may or may not include LMSmodular functions.
This example shows three operating stations connected with a local area network; two of them are connected to a gateway that controls access control panels.



3.7 Example 7: client/server

This example shows the solution found to optimize network traffic on Cerloop configurations: LMSmodular stations can be grouped in subsets connected through local TCP/IP-based networks. For each subset, a single LMS station identified as the “server station” can thus manage communication with the loop. All the other ones, identified as “client stations”, can get the field information from the server via the LAN connection.
For a given subset on the same LAN, only one station at the time can act as a server all the others must be clients.



4 System parameters

Parameter (max number of)	Value
LMSmodular system:	
sites	1000
systems	1000
subsystems	1000
points	999999
point property fields	10000000
treatment tables	1024
description tables	1024
reaction tables	9999
sequences	9999
time programs	9999
exception days (holidays)	200
single advisories	9999
advisory programs	9999
operators	255
windows applications	99
running windows applications	1
icons	65535
subsystem network addresses	10240
treatment pages	9999
foreground symbols per treatment page	50
foreground commands per treatment page	9
graphic slides (Graphic Station)	9999
foreground symbols per graphic slide	100
historic on-line records	From 16000 to 256000
guard tours	100
active guard tours	1
guard tour stations	200
guard tour stations per tour	40
guard tours per station	3
Access control parameters: (WSE only, see also CerPass documentation)	
users	8000
zones	unlimited
time zones	1024
panels	255
panels per serial line	16
historic on-line records	…
Optional devices:	
Parallel logging printers per LMSmodular station	1
Parallel graphic printers per LMSmodular station	1
Serial logging printers per LMSmodular station	1
Graphic station per LMSmodular station	1

Gateways:	
GW-20s per LMSmodular station	4 (2 with standard PC hardware)
GW-21s per LMSmodular station	4 (2 with standard PC hardware)
GW-21s and GW-20s (mixed) on the same LMSmodular station	possible
GW-21s per GW-20 at intermediate level	20
GW-20s via another GW-20 at intermediate level	not allowed
LMSmodular stations per GW-20	4
Subsystem lines per GW-20	20 (16 if either NISE or FHI Pad is installed)
LMSmodular stations per GW-21.04	2
LMSmodular stations per GW-21.06	2
Subsystem lines per GW-21.04 with one LMSmodular stations	3
Subsystem lines per GW-21.04 with two LMSmodular stations	2
Subsystem lines per GW-21.06 with one or two LMSmodular stations	4

Max Distance (typical)		
Connection Type	**Baud Rate**	**Max Distance (mt)**
GW-xx to subsystem	300	1000
GW-xx to subsystem /PC station	1200	300
GW-xx to subsystem /PC station	4800	50
GW-xx to subsystem /PC station	9600	15

Cable Specification: 22 AWG twisted pairs each shielded in Belden 8777 (three pairs) shield tied to ground

Siemens Building Technologies AG
Cerberus Division
CH-8708 Männedorf
Alte Landstrasse 411
Tel. +41 1 - 922 61 11
Fax +41 1 - 922 64 50
www.cerberus.ch

Cerberus
Security
for People
and Assets