SIEMENS

Cerberus® LMSmodular Basic Module Ver. 2.46

System Description

Fire & Security Products

Siemens Building Technologies Group

Document changes in Version 2.4

Topic	Comments
Presentation layer	Peer to peer and client/server architecture
Host interface	DDE and NetDDE
Subsystems	CC30 CerPass, as well as MM/MF and Transliner are now supported; CF9003 is now available and compatible with CMX; also, Siemens SiMatrix has been adapted to CDDL/CDSF
Hardware requirements	New hardware requirements for V2.43, V2.44
Software requirements	Windows 95/98, Windows NT for communication servers
Presentation level	Graphical navigation (Page Browser)
System parameters	Multi-station architectures DDE item specifications Larger historic database No more Access Control specifications: see CerPass specifications

1 Introduction

This document provides a brief description of the characteristics and features of the Cerberus centralised control system LMSmodular.
Its purpose is to give prospective customers and new users an overview of the comprehensive capabilities and features of this system.
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. It monitors both concentrated sites as well as sites that are connected by local and distributed networks.
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 what 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 NISE or FHI Pads, 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

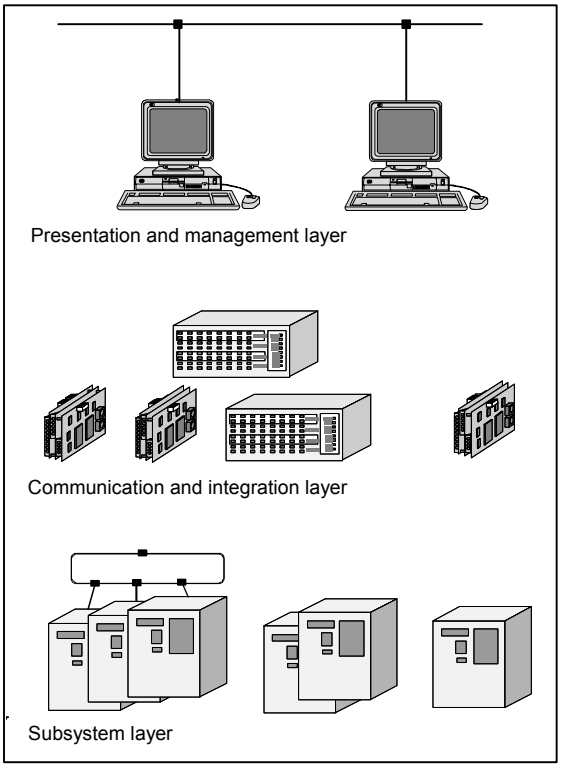
You can refer to the following Cerberus documents to have information about specific products mentioned in this document. In these manuals you will find also information about how to install and/or configure software and hardware parts needed to properly set up your system.

- GW21 Technical Manual e1481
- GW20 Technical Manual e1478
- NK822x Technical Manual e4414
- LMSmodular Installation Manual V2.46 e1862a
- LMSmodular User Manual V2.46 e1865a
- LMSmodular Configuration Guide V2.46 e1863a
- LMSmodular Configuration Reference V2.46 e1864a
- FHI Pad Engineering Guidelines e1143
- IMS2000 Engineering Guidelines e1142
- CDDL Cerberus Dati Data Link
  - Data Link Protocol Description e1152
- CDSF Cerberus Dati Standard Format
  - Application Protocol Description e1151
- LMSmodular Software Product description V2.4 e1866
- LMSmodular Application Examples V2.4 e1868

2 System architecture

A basic prerequisite for obtaining real benefits from security and protection systems is the reliability and availability. These benefits must not be impaired by the integration of the systems into a control centre. For this reason the system architecture of LMSmodular is based on the strategy to implement the available functions within an overall system as close as possible to their place of deployment or creation. This means, for example, that the interactions between the individual subsystems are not implemented in the control centre computer but in the lowest ranking, jointly used communications node of the corresponding subsystems.

In accordance with this concept, LMSmodular comprises 3 functional levels, with an optional network layer that links the Operating Stations.



This architecture is the most general and actually there are many configurations available. Some layers can be dropped, to answer specific needs, or can be duplicated to get redundant configuration. Even inside each layer more than one configuration can be implemented, according to the actual type of hardware installed and the configuration that the system engineer judges best fitted for the specific plant.

2.1 Subsystem layer

It is the lowest level. It includes all local control units of the connected systems, i.e. control units such as CZ10, CZ12, CS4, CS11, CC60 etc. and their sensors and actuators.

All these subsystems have in our architecture complete functional autonomy from upper layers, so that the field operations and a satisfactory level of security can be guaranteed even in case of failure of the layers above. For instance the intrusion system will be able to transmit vital alarms to police without intervention of the upper layers, while access granting will be managed autonomously by the access control controllers.

The control units can be connected to the nearest higher layer, i.e. the communication and integration layer, either directly or in a loop.

When there is a direct connection, each control unit has an independent communication link with a Gateway in the communication and integration layer.

Two or more control units however can be connected in a loop, a sort of local network. In this case more than one control unit share a single communication channel toward the upper layer. A loop master, or concentrator, takes charge to manage the data flow to and from the subsystem layer.

2.2 Communication and integration layer

This layer consists of the actual communication network and one or several communications controllers, called gateways. The gateways fulfil 3 principal tasks:

- Interpret and translate the various communications protocols from the different control units
- Concentrate the data flow between the upper and lower layers
- Manage the interactions between subsystems.

It is quite common in real-world installations that the different subsystems are implemented in different times by different suppliers, which implies that different communication protocols are used. The Gateways solve the first problem, communication and protocol conversion, because they are able to communicate with the various control units, allowing moreover an homogeneous connection to the presentation layer.

In an integrated safety/security system, the different subsystems have to interact among themselves in order to provide global services. Examples of such interactions are for instance well known functional links between intrusion and CCTV switching matrix, but also among fire and technological plants, fire and access control and so on.

Such interactions are part of the real time operation of the system, they require high speed, as in the case of triggering a CCTV camera by a volumetric intrusion detector, and high reliability, as they often involve safety functions. Therefore, they have to be structurally implemented as low as possible in the system architecture. In our solution therefore these functions are directly realised in the network components, and do not require any intervention of the presentation layer.

The communication and integration layer cannot be considered just a passive communication infrastructure. It has a very active role into maintaining the communications alive and fully monitored. It can diagnostic any communication fault and immediately reports the anomalous conditions to the upper layers.

It keeps the communication secure, if required, by encrypting the transmitted data and decrypting the received information to make them accessible to the underlying control units.

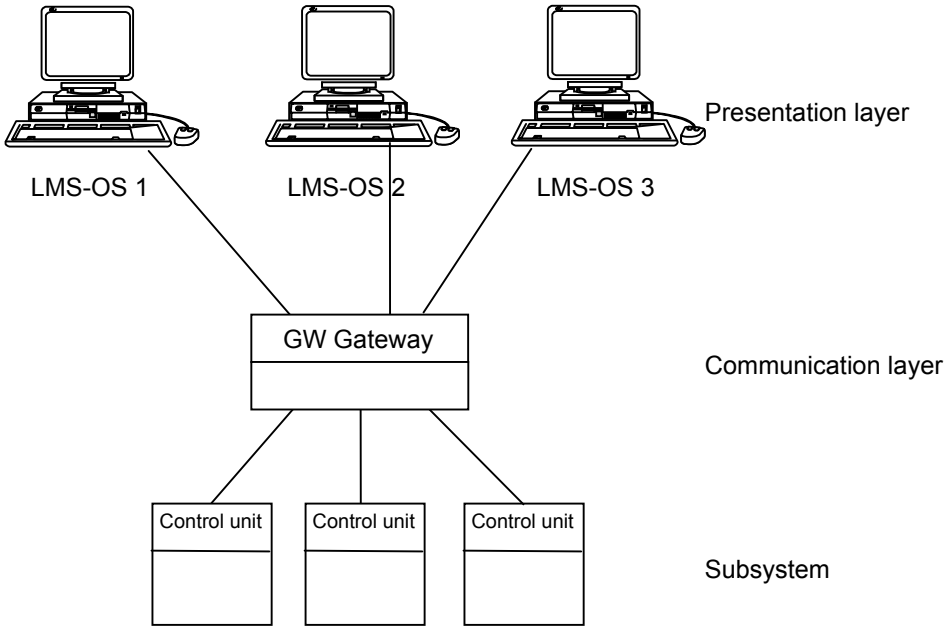
Different architectural solutions can be implemented at this layer to adapt the LMSmodular to your actual plant layout. The communication and integration layer is described in detail in Chapter 4 of this document.

2.3 Presentation and management layer

The presentation and management layer is the layer at which the information are organised and displayed to the operator. At this level, moreover, the user can interact with the whole system either managing the devices connected to it or configuring the system itself.
Thanks to the distribution of time critical functions to the network layer, the presentation layer can operate without the constraints of real time operation.
The interaction is performed using the LMSmodular Operating Station, i.e. a PC on which LMSmodular is running, with the proper PAK (Program Authorisation Key) installed and activated.
The PC running LMSmodular becomes fully dedicated to the system management and becomes an Operating Station (LMS-OS). The functions available on the Operating Station depends on the software license purchased and ranges from the basic functions of the LMSmodular base module up to the full functions that include Access Control and Guard Tour management.
At the presentation and management layer belongs the Graphic Station (LMS-GS) too. The LMS-GS can be used only in conjunction with a standard OS and it implements only the presentation functions. It does not allow the operator to interact with the system and therefore it does not implement the management functions.

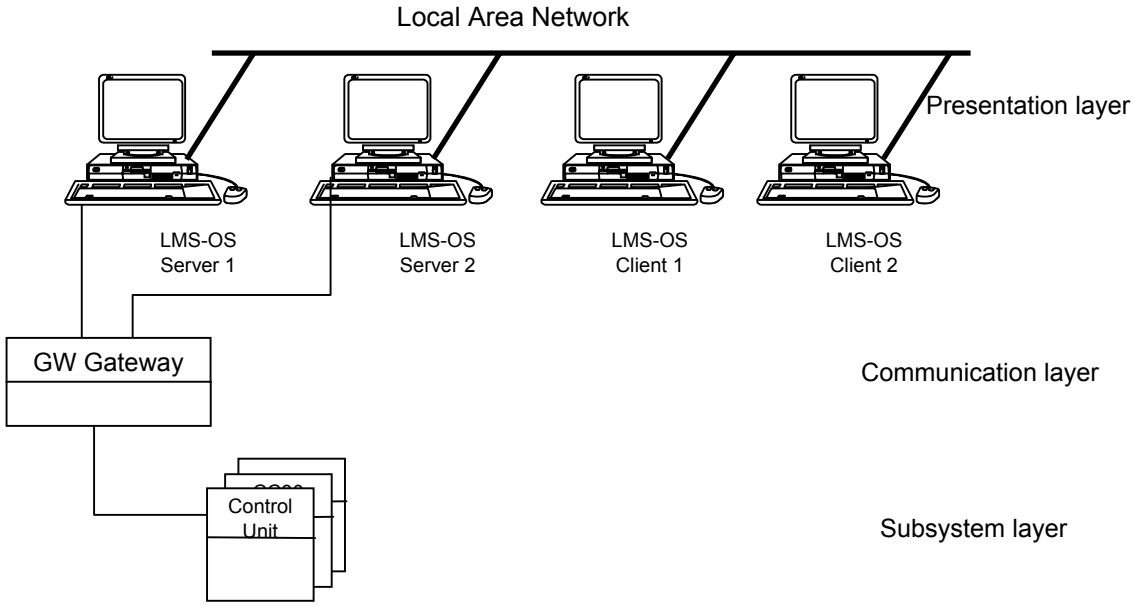
2.3.1 Peer to peer architecture

LMSmodular normally adopts a peer-to-peer architecture that allows the connection of the Operating Stations directly and independently to the communication and integration layer, so to achieve a very high functional autonomy and a very high reliability of the overall system.
In this configuration, the unavailability of the LAN that connects the Operating Stations does not affect their performances, thanks to the LMSmodular direct connection of all the workstations to the field via independent communication lines.
This architecture has been chosen in order to obtain a higher system reliability at lower costs and easy scalability.



2.3.2 Client/server architecture

The Operating Stations can optionally be interconnected and exchange information through a Local Area Network. When several LMSmodular workstations are used in a system, they can in facts be connected to a LAN in order to allow a client/server architecture.
LMSmodular supports standard LANs, and in particular both Ethernet and Token ring. One station in the pool of serves takes over the communication task and provides for the connection services for the other server and client stations. The role is assigned dynamically and may change in case of failure of one station, so as to assure complete reliability.
The client stations can operate without direct connection and get a faster refresh of the field status via network messages.



3 Field

LMSmodular can integrate different subsystems by interpreting and converting their protocols. When these subsystems are connected to the system, the events they generate are displayed in a homogeneous and consistent way . Moreover they can be managed from the LMSmodular Operating Stations with the same user interface, although the actual management pages reflect each subsystem's peculiarities.

3.1 Supported subsystems

LMSmodular manages the following subsystems:

Subsystem	Description
Cerberus CZ10/CS11	fire detection
Cerberus CZ12/CS4/CS440	intrusion detection
Cerberus CC60	gas detection
Cerberus CB100	synoptic panel
Cerberus MK7022/CK100	concentrator units for Cerban control panels connected in a Cerloop configuration
Cerberus CC30	access control door controller
Cerberus MM / MF	input / output units
Cerberus Dati CMX/CF9003	digital I/O multiplexing system
Cerberus Guinard STT	fire detection system
Cerberus Transliner	intrusion detection
CBA Fire detection panels	fire detection system
Siemens SiMatrix CCTV	closed circuit television matrix
Comerson CCTV	closed circuit television matrix
Burle CCTV	closed circuit television matrix
Westinghouse SE 422,818,4100	access control systems (phase out)

3.2 Third part subsystems integration

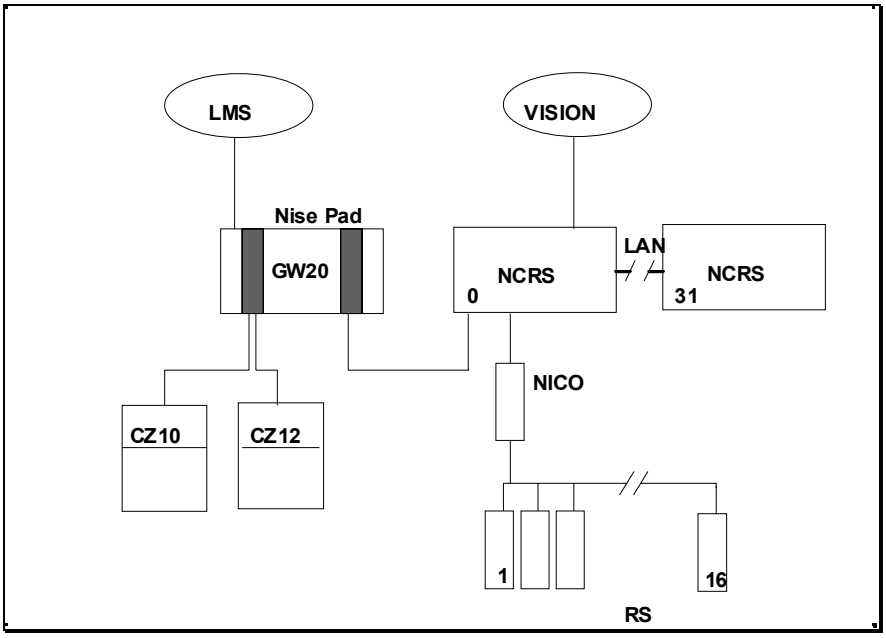
LMS was developed on the purpose to integrate different protocols. No wonder therefore that LMSmodular is able to integrate devices designed and manufactured by third part producers, that communicate using their own protocol.
LMSmodular is however an open system, that communicates with a public protocol called Cerberus Dati Standard Protocol (CDSP), composed by a data link layer (CDDL - Cerberus Dati Data Link) and an application level (CDSF - Cerberus Dati Standard Format). Any third part manufactures can produce devices that communicate using this protocol and therefore that can be immediately integrated into and existing LMSmodular system.
Two different subsystems are foreseen for integration:

- IMS2000, that allows the integration of Staefa Control MS 2000 technological plant control device;
- any third part CDDL/CDSF-compliant device

Any other subsystem can be virtually integrated into LMSmodular, beyond these two, but this could require some additional software development and therefore must be evaluated on a per-case basis.
An LMSmodular based system moreover can exchange messages with a supervisor system other that LMSmodular itself. This is performed using an FHI Pad. This Pad must be inserted in a Gateway's slot and it allows integration of a Foreign Supervisor System, developed by third parties.
Also, the DDE and NetDDE Windows protocols can be used by LMSmodular for the real-time data exchange with other Windows applications, local or networked.

3.2.1 IMS 2000

IMS2000 is a system designed to integrate technological and security plant management systems. It does not replace either the existing security system or the existing technological plant management system. It links the technological plant items to the security system and it links the security points to the technological system.
IMS2000 is based on two already marketed and well established products: Cerberus' LMS and Staefa's MS2000. The first manages security systems, the second technological plants. Both use a front-end processors, called Gateway GW20 in the Cerberus' LMS System and NCRS in the Stäfa MS2000 system. Adding a dedicated piece of hardware (the NISE Pad) and the firmware residing on it, to GW20, you can send security messages to NCRS and receive from it technological messages.
The scheme shows the system architecture.



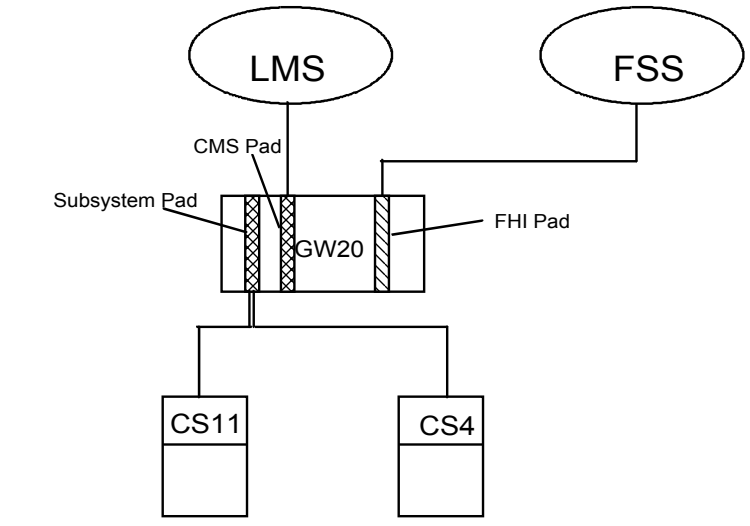
The integration between the two systems is performed at Gateway-NCRS level. Cerberus Dati developed a specific electronic board that can be plugged in a Gateway's slot and it is called NISE Pad. The NISE Pad has a serial port a NCRS can be connected to. By this link, a communication is established between LMS and MS2000: the two previously separated systems are now integrated and they are called with the collective name of IMS2000.
The NISE Pad contains firmware that lets you convert data in the format used by NCRS to the format used by LMS and conversely converts data from LMS to NCRS in order to let the two systems to understand each other. Moreover, the NISE Pad contains firmware that can be configured to perform interactions among the security/safety subsystems and the technological plant items installed.
The actual system can be configured without either the LMS or the VISION monitoring station (but not without both of them !). If one of the two monitoring station is not installed, the monitoring capabilities are somewhat limited. For instance, the operator working on an IMS2000 system equipped with an LMS only will be able to detect the alarms coming from analog technological item but he will not be aware of the analog value measured.

3.2.2 FHI Pad

FHI Pad is an interface that allows the Cerberus danger management system to transfer real time information regarding its status to a supervisor system other than Cerberus' LMSmodular, named Foreign Supervisor System (short FSS). The FHI Pad interface allows the Cerberus danger management system to receive commands from a Foreign Supervisor System.
The same interface could also be used vice versa to allow a LMS system to receive information and to send commands to a FSS.
The interface is not designed for file transfer; therefore historic or statistical data will not be available through it.
The interface adopted complies with Cerberus norm VT397e, "Communication of a danger detection system with a higher ranking system".
The FHI Pad functions are:

- to allow an LMSmodular system to access a subset of the information points of a non Cerberus *FSS* system. The LMSmodular system will therefore be able to receive selected changes of status and to issue selected commands to the specified FSS point subset.
- to allow an FSS system to manage a subset of the information messages of Cerberus control panels (CZ10, CZ12, CS4, CS11, CC60). FSS will therefore be able to receive selected changes of status and to issue selected commands to Cerberus control panels.
- to allow automatic interactions between security subsystems connected to the LMSmodular gateway and the technological devices connected to the FSS.

The Foreign Supervision System is a system supplied by a third-part manufacturer that should monitor a technological plant, to be integrated with LMS security and safety monitoring system.
The FSS should comply with Cerberus Dati Standard Protocol (CDSP) specification and it will be seen by LMS as a standard subsystem. FHI Pad behaves as slave, while FSS behaves as master. Both the application level (CDSF) and the data link level (CDDL) of the CDSP protocol are needed by FHI Pad.



The FHI Pad that implements the interface functions is composed by a hardware board to be inserted in the Cerberus' Gateway GW20 and a software package to be installed in an EPROM bank on the board.
The FHI Pad is therefore an extension of GW20 capabilities and it is sold as an add-on device to standard Gateway GW20.

3.2.3 Windows DDE and NetDDE

Connection to third party systems can also be realised via the Windows DDE / NetDDE protocols. This solution allows real-time data exchange between the Cerberus danger management system and a third-party supervisor system.

DDE

The Dynamic Data Exchange (DDE) provides the ability for Windows-based applications to dynamically exchange information. All Windows versions include the support for Dynamic Data Exchange.

DDE is a message protocol that can be used for exchanging data between Windows-based applications. When used in an application, DDE offers the user a more integrated Windows work environment. For technical information about the DDE, see the Microsoft Windows Programmer's Reference, Volume 1.

DDE is most appropriate for data exchanges that do not require ongoing user interaction. Usually, an application provides a method for the user to establish the link between the applications exchanging data. Once that link is established, however, the applications exchange data without further user involvement.

Certain concepts and terminology are key to understanding dynamic data exchange. The following sections explain the most important of these.

DDE Client, Server, and Conversation

Applications participating in dynamic data exchange are engaged in a DDE conversation. The application that initiates the conversation is the client application; the application responding to the client is the server application. An application can be engaged in several conversations at the same time, acting as the client in some and as the server in others.

LMSmodular can, with appropriate configurations, act both as server and client in DDE conversations.

Application, Topic, and Item Names

DDE identifies the units of data passed between the client and server by using a three-level hierarchy of *application*, *topic*, and *item* names.

Each DDE conversation is uniquely defined by the application name and topic. At the beginning of a DDE conversation, the client and server determine the application name and topic. The application name is usually the name of the server application, for LMSmodular the application name is “LMSRTDB” (LMS Real Time DataBase).

The DDE topic is a general classification of data within which multiple data items may be discussed (exchanged) during the conversation. For LMS modular, the topic is a subsystem and the topic name is a label assigned to the subsystem at configuration time.

A DDE data item is information related to the conversation topic that is exchanged between the applications. The data item for LMSmodular is a point representing an object (each item name is assigned to the points at configuration time). Values for the data item can be passed from the server to the client or from the client to the server in two possible scenarios:

1. LMSmodular acts as DDE server: it provides to DDE clients the value of items representing the information messages of Cerberus control panels (CZ10, CZ12, CS4, CS11, CC60) and can receive new values of items that are intepreted as control actions for the addressed objects.
2. LMSmodular acts as DDE client: it receives, via DDE messages, the changes of status of the DDE server that are mapped on internal LMSmodular points and it can issue selected commands to the specified points.

Important: a max of 800 items can be exchanged with LMSmodular.

NetDDE

Network DDE takes all of the capabilities of DDE as explained earlier in this chapter and extends this powerful capability across a LAN (Local Area Network) to allow applications on two workstations to dynamically share information. Network DDE is not a special form of DDE; rather it is a redirector that runs in the background on a Windows workstation searching for particular information contained in a DDE conversation.

In order for an application on a Windows workstation to use Network DDE to communicate with an application running on another workstation, a DDE share must first be created. A DDE share is analogous to a file share or a printer share as defined in Windows and is used to specify the security permission-levels that grant remote users access to DDE information on the local workstation. The DDE share is used to prevent applications that support DDE from gaining unauthorized access to the local workstation.

Network DDE is implemented as a Windows-based application (NETDDE.EXE) that runs in the background of the Windows workstation, and should be loaded by the Windows at startup. Because Network DDE is an application that is not visible to the user, Network DDE doesn't appear in the Windows Task List while it is running.

LMSmodular can profit of NetDDE services and provide the same functions available with local DDE. The configuration settings of the application, topic, and item names, although slightly different, are conceptually the same as the ones for DDE described above.

4 Communications level

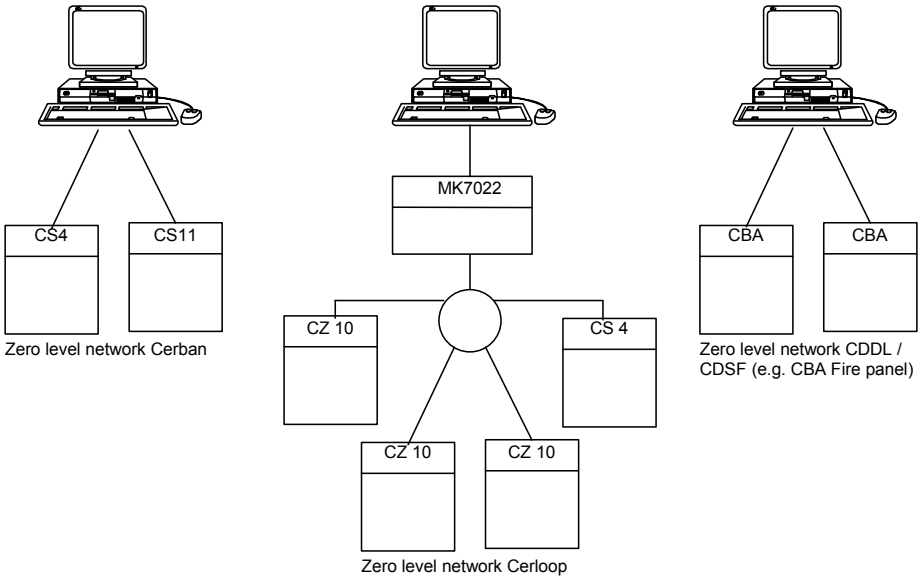
4.1 The LMSmodular network solutions

There are five types of network architectures:

- **zero level network** : the subsystem is connected directly to the operating station
- **one level network**: at least one gateway is interposed between the operating station and the subsystems
- **two level network** : there are at least one gateway with the role of concentrator and one gateway at a lower hierarchical level. This last gateway is directly connected to the subsystem(s)
- **redundant configuration**
- **multiple gateway configuration**

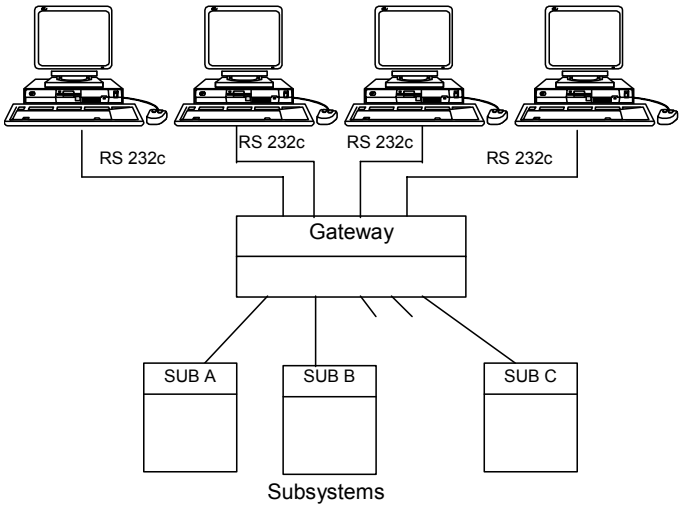
4.1.1 Zero level network

It is the simplest network architecture available. The subsystem is directly connected to the operating station through a serial line. No GW-type network device is interposed.



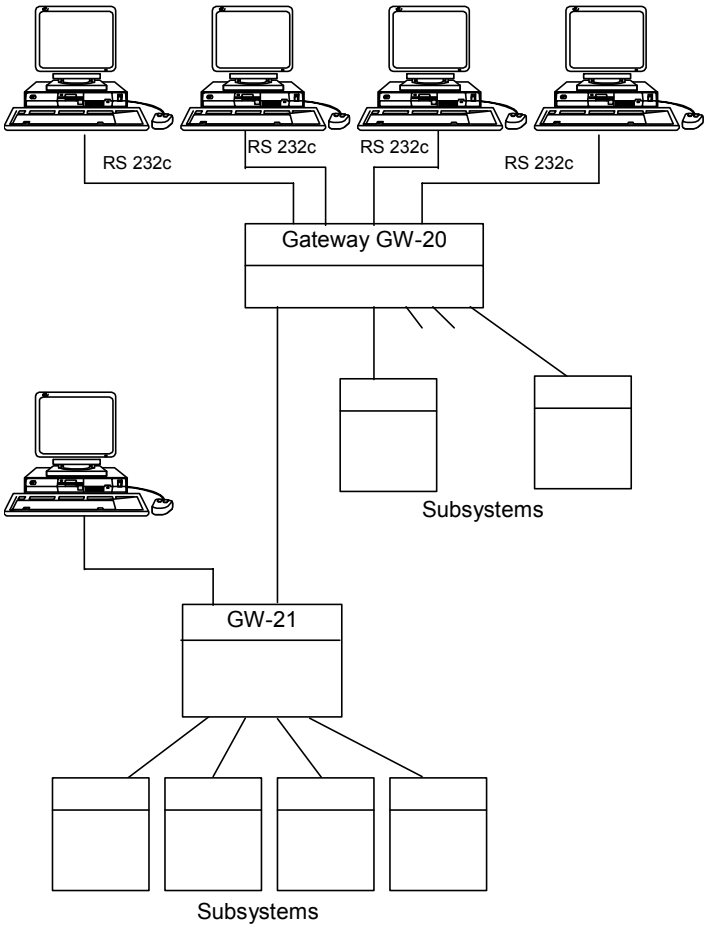
4.1.2 One level network

In this network the operating station(s) are connected to the Gateway by serial lines. The messages are exchanged on this line using the CDDL/CMSDF protocol, a proprietary protocol by Cerberus Dati. The gateway could be as well a GW20 or a GW21.
The gateway is the data concentrator that receives messages from the subsystems connected to it and sends them the commands issued by the operating station. The communication on the lines that run from the Gateway to the subsystems is performed with the protocol specific of each subsystem.



4.1.3 Two level network

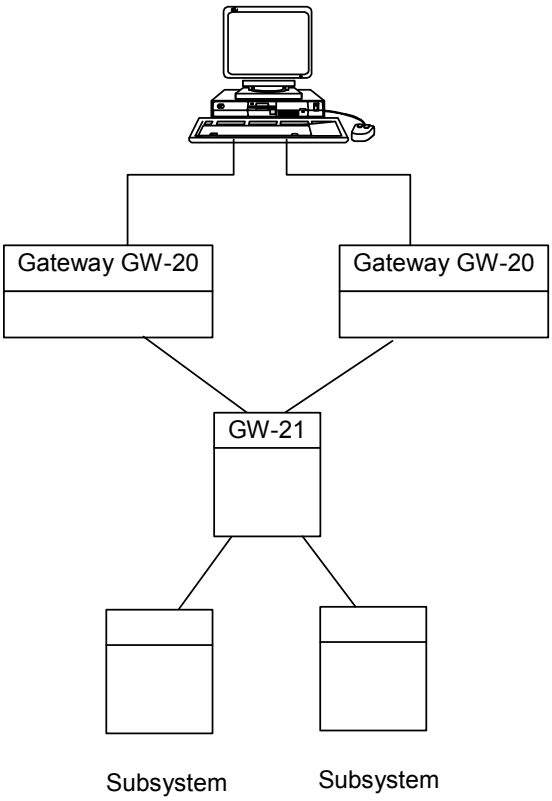
The two level network includes at least one Gateway GW20 with the role of concentrator and one or more GW21 subordinated to it (second level gateways).
The presence of a two level network does not exclude the contemporary presence of subsystems directly connected to the gateway that acts as a concentrator.



The communication between the second level gateways and the concentrator is performed using the CDDL/CMSDF protocol.
The two level network is particularly suited for wide area plants. The second level gateways can for instance control small and medium sites equipped with up to four subsystems. These sites refer to a supervision centre, located somewhere and reached through a dedicated communication line where the concentrator gateway communicates with the operating station(s).
To protect the data against tampering, the Gateway can encrypt data enabling cryptography option both between the operating stations and the GW20 and between GW20 and GW21. When the cryptography is enabled, the data are scrambled using an encryption algorithm that periodically changes. To enable the cryptography, the Gateway GW20 and / or the operating stations must be equipped with a master key that contains random numbers. Everyday, a session key is generated and distributed to the lower level gateways. Because the session key is generated from a random set of numbers, no repetitive pattern of session keys can be detected even on a long time interval. The session key is used to scramble the messages transmitted only during that day, and it is changed the day after.

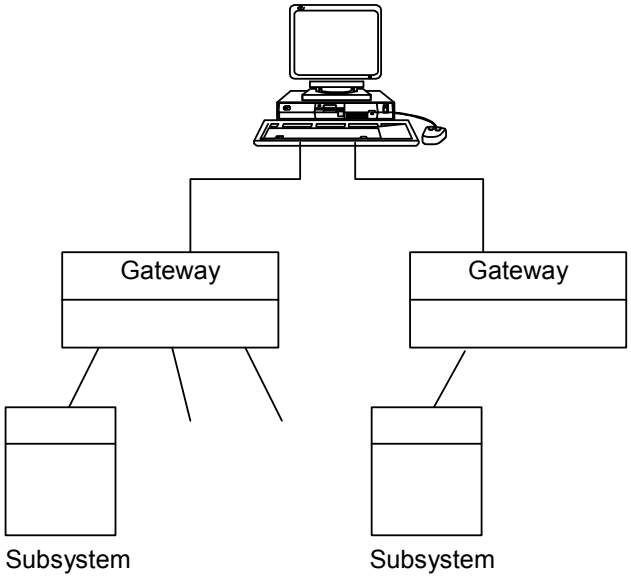
4.1.4 Redundant configuration

In the redundant configuration a single LMSmodular Operating Station is connected to two gateways. Each one of them receives the messages generated by the same control panel. The data path from the control panel to the Gateway is therefore duplicated and it allows to obtain a higher security degree. Should a communication path fail, the other one is still available to send messages upward and transfer commands downward.



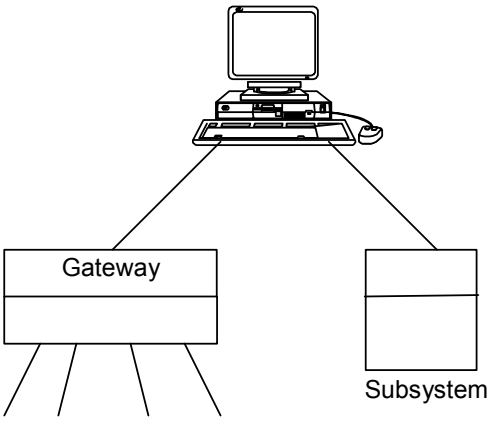
4.1.5 Multiple gateway configuration

The multiple gateway configuration is used when the number or location of control panels compels to use more than one gateway. For instance, if you have installed more than 20 control units with point-to-point connection, the 20 lines of a single gateway GW20.20 are saturated and you must install one more gateway. The two gateways are connected through two separate serial lines to the same LMSmodular Operating Station.
Gateways can be of different type (e.g.: one GW20 and one GW21)



4.1.6 Mixed Configuration

In the mixed configuration to a PC can be connected both a gateway of any kind (e.g. GW20 or GW21) and a subsystem with direct connection.



4.1.7 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.

4.2 Subsystem connectivity

Subsystem	Protocol	Zero-level	One-level	Two-level
Cerberus CZ10/CS11	CerBan/CerLoop	Yes	Yes	Yes
Cerberus CZ12/CS4/CS440	CerBan/CerLoop	Yes	Yes	Yes
Cerberus CC60	CerBan/CerLoop	Yes	Yes	Yes
Cerberus CB100	CerBan (GW20)	N/A	GW20	N/A
Cerberus MK-7022/CK 100	ISO-1745	Yes	Yes	Yes
Cerberus CC30	CerTalk	Yes	Yes	Yes
Cerberus MM / MF	CerBan/CerLoop	Yes	Yes	Yes
Cerberus Dati CMX/CF-9003	CMX-DL	No	Yes	Yes
Cerberus Guinard STT	CerLoop	Yes	Yes	Yes
Cerberus Guinard STT	CerBan	No	GW21	No
Cerberus Transliner	Size	No	Yes	No
CBA Fire detection panels	CDDL-CDSF	Yes	Yes	Yes
Siemens SiMatrix CCTV	CDDL-CDSF	Yes	Yes	Yes
Comerson CCTV	CDDL-CDSF	Yes	Yes	Yes
Burle CCTV	Allegiant CCL	No	Yes	Yes
Westinghouse SE 422, 818, 4100	SEEP 4.1	Yes	Yes	Yes

4.3 Gateway functions

In addition to its primary function as a data concentrator between several subsystems and one or more PC station(s), the gateway(s) perform(s) a number of supplementary functions within the centralization system. Specifically these are:

4.3.1 Protocol translation

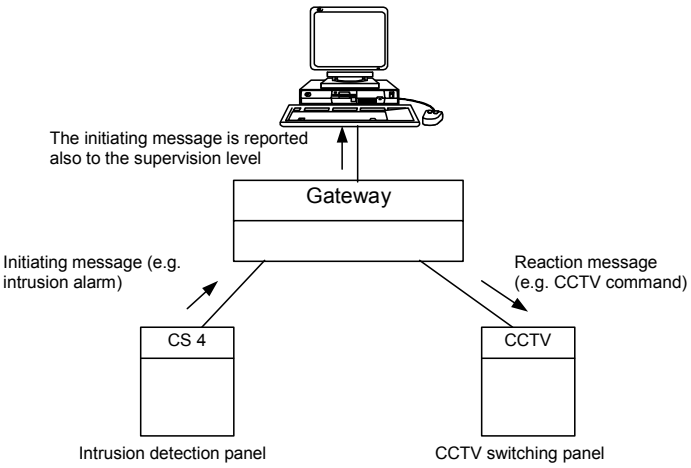
The transmission protocols transmitted by the various subsystems or system groups are translated by the gateway into a uniform protocol. The structure of the messages remain unchanged.

4.3.2 Time management

The subsystems are synchronized with the system time every hour by the master station via the gateway. The gateway provides for time stamp on messages which do not already have it in the native protocol format.

4.3.3 Interactions

Interactions are configured on the Gateway and performed at network level. The interactions supply a fast and reliable way to link the occurring of some set of conditions with an automatic answer by the system. The reactions are fast, because they are dealt with at the gateway level without delays introduced by communication with higher system levels. The gateway is a multiprocessor environment, that deals with events in a real time mode. Moreover, the interactions are highly reliable because they are undertaken at the lowest level possible in the system. The highest system level (i.e. the PC operating station) is not involved at all in the interaction triggering - although it is kept constantly informed of what is going on.



4.4 Logging

A log printer can optionally be connected to the gateway GW20.xx (see following section). This printer documents in plain text the complete telegram traffic of the corresponding gateway.

4.5 Hardware

For the gateways two different hardware versions are available:

- **GW21**. Up to two operating stations can be connected to it. It manages up to 4 subsystems. There are some limits on the subsystems' mix you can connect. The protocol configuration on GW21 is usually performed by jumpers.
- **GW20**. Up to 4 operating station can be connected to it. It manages up to 20 subsystems (less when some other options are selected, please refer to the “System Parameters” section). There are virtually no limits on the subsystems' mix you can connect, but there are limits on the subsystems type you can connect to a single Subsystem Pad. It can be integrated with technological plants. It can be connected to a foreign supervision system as well as with foreign subsystems, i.e. with systems or subsystems manufactured by third party but compliant with CDI specifications (CDDL/CDSF protocols). The protocol and routing configuration on GW20 is performed by EPROM.

4.5.1 GW21.xx

This single-processor version features 4 to 6 communications channels and is principally intended for smaller systems comprising up to 4 subsystems and 1 or 2 control centre computers. In large systems, the GW21 can be used together with the GW20 to implement a two level network. The GW21 consists of one or two circuit boards to be installed on a base module. It can be mounted directly into the subsystem to be connected which normally also supplies the power for this module.
The configuration can be defined directly with jumpers.

Fig. 1 GW21

4.5.2 GW20.xx

The GW20 is a modular unit built in 19" technology from identical communications boards. Each communications board features 4 serial channels and a dedicated 8-bit processor.
This gateway is used in medium to large installations and can manage up to 24 standard communications channels (20 subsystems and 4 control centre computers), plus special channel for logging printer / synoptic panel (CB100).
By plugging in additional communications boards the gateway can be expanded step by step from 4 to 20 communication, channels for subsystems.
In addition to the standard board for subsystems (sub pad), two special communication boards are available. These differ only in the control software stored in the firmware EPROM:

- The FHI pad supports the connection of LMS to an external host system.
- The NISE pad establishes the connection to the MS 2000 building automation and management system of Staefa Control.

A power pack for connecting the unit to 230 VAC or a DC/DC converter is also available and can be installed in the 19" housing.
The GW20 gateway parameters are set with a special configuration tool. With this convenient, menu-controlled tool all necessary parameters, including interaction programs, can be generated.
The configuration files are stored in an EPROM in the gateway. If the gateway is equipped with a non-volatile RAM (option), the data can also be loaded via a serial link directly from the service PC into the RAM.

Fig. 2 GW20

5 Presentation and management layer

A detailed description of the LMSmodular software that runs on either the LMS-OS or LMS-GS is supplied in the document “LMSmodular Software Product description”.
In a LMSmodular installation there are two types of workstation:

- the Operating Station (LMS-OS). It displays information about the system and lets the user interact with it. The operator can treat the events or send commands to the installed devices, for instance, in both text and graphical way. At least one Operating Station must be installed in each LMSmodular-based plant.
- the Graphic Station (LMS-GS). It is always linked to an Operating Station. The LMS-GS displays graphic pages, called maps, when an event arises. It simplifies the event assessment and counteracting by the operator. It has neither keyboard nor mouse so it is just an output device associated to the LMS-OS.

5.1 Operating station

From the operating station the operator can

- manage the field events and properly treat them
- send commands to the control panels installed in the field and verify their proper operation
- manage the historical archives (store data and lets the operator retrieve them)
- navigate through graphical pages reporting, at multiple level, the real-time state of field objects
- configure the plant to keep it updated with possible hardware modifications

The link between the operating station and the network must be a dedicated serial line, permanently available.

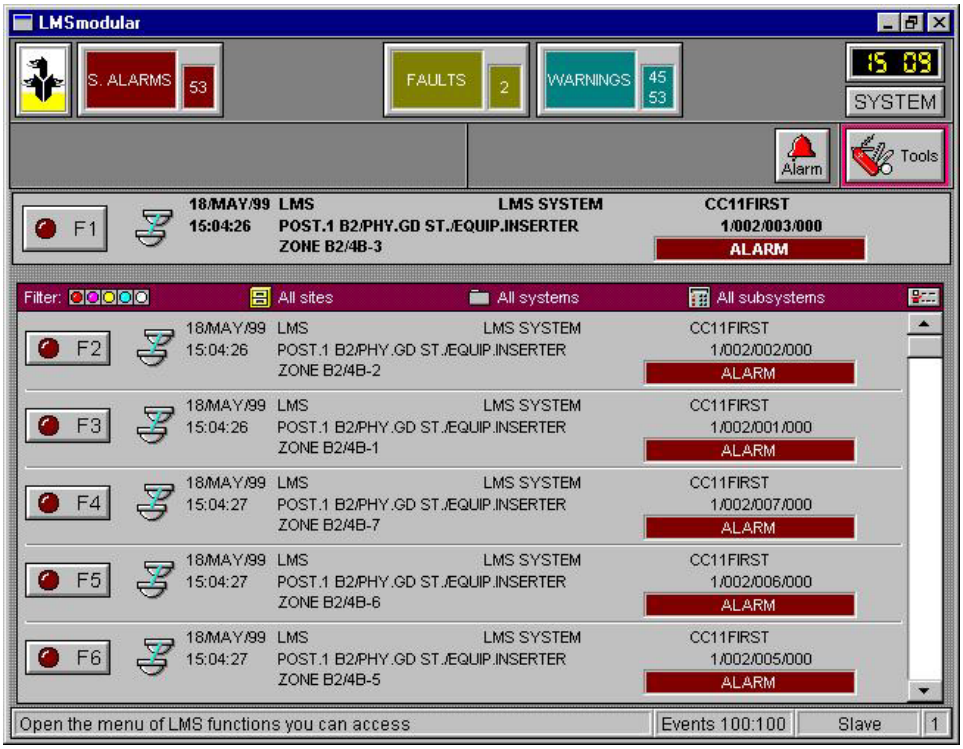


Fig. 3 LMS user interface: event list

5.1.1 Hardware requirements

The Operating Stations are based on an industry-compatible Personal Computer.

- CPU and RAM memory: see Tab. 1
- keyboard
- VGA adapter, supporting 64K colors or more at 640x480 and monitor
- floppy disk drive configured as A: (3.5" 1.44 MB)
- CD-ROM drive
- serial interface (COM1: and optionally COM2:)
- hard disk drive C: minimum 500 MB

In addition the workstation should be configured with:

- a printer for logging the events and operator activities.
- a graphic printer to print out maps and schemes
- a sound card (Windows compatible), that emits a loud sound when there is an incoming event
- a serial printer, as an option to the parallel printer
- a local network adapter, for NetDDE connections and LMS-GS

The printers, both serial and parallel, are used to log on paper all the events from field and operator actions that occur during the LMSmodular operation.

LMSmodular supports the use of a graphic printer to reproduce on paper the screens. You can use a colour printer to get colour hardcopies.

Although the screen resolution of LMSmodular is 640 x 480 pixels x 64K colours, the use of a large screen (17" or 21") could improve the system. The video must comply with both hardware and software VGA standards.

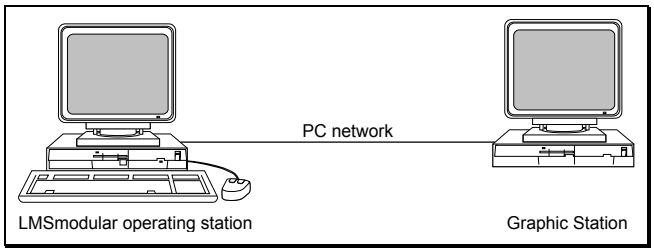
5.1.2 Software requirements

LMSmodular runs under MS Windows 95/98. In the client/server solution, servers can be installed under Windows NT, although limiting some client functionalities.

Because LMS is designed as a security system, some functions that are normally available in Windows are disabled by LMS.

5.2 LMSmodular Graphic Station

The Graphic Station is an output device designed to work in conjunction with LMSmodular, the centralised monitoring system by Cerberus Dati.
The Graphic Station displays graphic maps when an event occurs, and by doing so it eases the operator's task to recognise the event and to perform the required actions.
A Graphic Station is a PC connected by a local network to the LMS operating station and running the Graphic Station program in the Windows environment. The local network hardware could be any among those that are fully Windows compatible.



When the operator treats an event or manages a subsystem, the Graphic Station displays the map configured for that event. The local network is the physical link between the two PCs and it is managed by Windows network services
When there is no operator active on the LMSmodular Operating Station, the Graphic Station shows an introductory map. This map could be used to display a logo, or a general representation of the controlled site.
When the operator treats an event, the map related to the event/point is shown. For each point status, up to five pages can be configured. The fifth page is the map to be displayed when that status for that point occurs.
During subsystem management, the Graphic Station displays the map configured for the subsystem.
Graphic station is supported in two different versions:

- Graphic Station standard (or shortly LMS-GS), supporting graphic maps at VGA resolution, the same as LMS Operating Station
- new Cerberus Graphic Station (or shortly LMS-CGS), supporting higher resolutions, map zooming and panning, direct import of AutoCAD drawings.

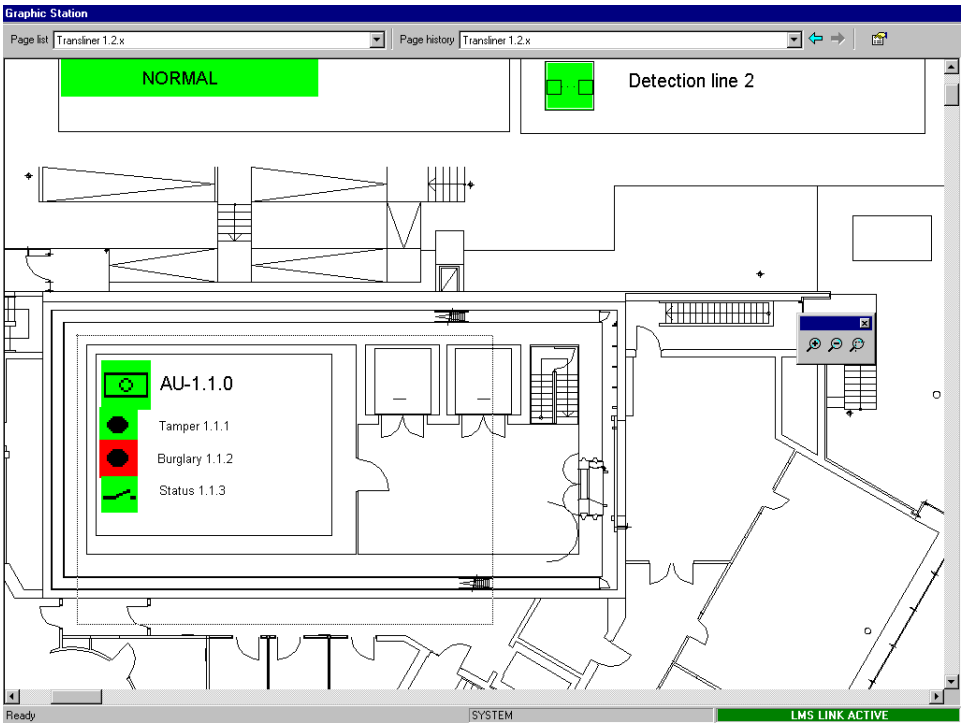


Fig. 4 CGS user interface

5.2.1 Hardware Requirement for Graphic Station

- CPU and RAM: see Tab. 2
- GS: VGA adapter, supporting 64K colours or more, and monitor
- CGS: SVGA adapter or better, supporting 64K colours or more
- floppy disk drive configured as A: (3.5” 1.44 MB)
- CD-ROM drive
- LAN adapter and software compatible with Windows
- hard disk drive C: min 500 MB

5.2.2 Software requirements

Standard LMS-GS runs under MS Windows 95/98.
New CGS requires Windows NT.

5.3 PC hardware configurations

LMS-OS versions and modules (1)	Pentium 133 MHz 32 MB RAM	Pentium 200 MHz 32 MB RAM	Pentium 300 MHz 64 MB RAM	Pentium II 400 MHz 128 MB RAM	Pentium III 500 MHz 256 MB RAM
V. 2.41 – Win 9x no LAN no CerPass no ACW	Recommended (3)				
V. 2.41 – Win 9x with ACW	Minimum (3)	Recommended (3)			
V. 2.41 – Win 9x with CerPass	Minimum (3)	Recommended (3)			
V. 2.43 – Win 9x V. 2.44 client – Win 9x		Minimum (4)	Recommended (5)		
V. 2.44 server – Win NT			Minimum (5)	Recommended (6)	
CGS - Win NT/2000			Minimum	Recommended	
V. 2.46 – Win NT/2000			Minimum		Recom-mended

Tab. 1 LMS Operating Station

Notes:
1. Guard Tour module does not affect the hardware requirements.
2. 16 MB of RAM memory can provide support for up to 10.000 points. Above that limit (and up to 30.000 points) install 32 MB.
3. 32 MB of RAM memory can provide support for up to 30.000 points. Above that limit, (and up to 65.000 points) install 64 MB. Above 65K points, contact support.
4. 32 MB of RAM memory can provide support for up to 10.000 points. Above that limit, (and up to 65.000 points) install 64 MB. Above 65K points, contact support.
5. 64 MB of RAM memory can provide support for up to 30.000 points. Above that limit, (and up to 65.000 points) install 128 MB. Above 65K points, contact support.
6. 128 MB of RAM memory can provide support for up to 65.000 points. Above that limit, contact support.

LMS-GS versions	Pentium 166 MHz 32 MB RAM	Pentium 200 MHz 64 MB RAM	Pentium 400 MHz 128 MB RAM
GS V2.4 - Win95/98	Recommended		
CGS V2.4 – WinNT		Minimum	Recommended

Tab. 2 Graphic Station

6 System parameters

Parameter (max number of)	Value
LMSmodular peer to peer / multi-station:	
LMS-OS Stations with GW20	4
LMS-OS Stations with GW21	2
LMSmodular client/server:	
Networked stations (total of servers + clients)	8
Communication server stations	4 (2 with GW21)
Communication client stations	7
LMSmodular database:	
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
DDE/NetDDE items	800
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
Optional devices:	
Parallel logging printers per LMSmodular station	1
Parallel graphic printers per LMSmodular station	1
Serial logging printers per LMSmodular station	1
Sound card per LMSmodular station	1
Graphic station per LMSmodular station	1

Gateways:	
GW20s per LMSmodular station	4 (2 with standard PC hard-ware)
GW21s per LMSmodular station	4 (2 with standard PC hard-ware)
GW21s and GW20s (mixed) on the same LMSmodular station	Possible
GW21s per GW20 at intermediate level	20
GW20s via another GW20 at intermediate level	Not allowed
LMSmodular stations per GW20	4
Subsystem lines per GW20	20 (16 if either NISE or FHI Pad is installed)
LMSmodular stations per GW21.04	2
LMSmodular stations per GW21.06	2
Subsystem lines per GW21.04 with one LMSmodular stations	3
Subsystem lines per GW21.04 with two LMSmodular stations	2
Subsystem lines per GW21.06 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

Documentation Evaluation Form

Please fax this form to

Siemens Building Technologies, Cerberus Dati Division Customer Support
fax n° + 39 02 45 28 19 33
from
Company _____
Name _____
Fax n° _____ **phone n°** _____

Please tell us how we did

	1 very poor ←		3 Medium		→ 5 very good	
General	**1**	**2**	**3**	**4**	**5**	**Do not know**
1. Organization of the LMS manual set						
2. Correctness of the contents						
3. Clarity and completeness (do the manuals explain clearly and thoroughly the concepts?)						
4. Punctual delivery of latest version						
5. Consistency with software releasess						
Easiness and effectiveness of use						
1. How easy is it to find information in the manuals?						
2. Are the manuals useful?						
Presentation of the documents, Quality of:						
1. Paper copies						
2. Binders						
3. Page formatting						
4. Pictures						
Document evaluation						
1. LMSmodular installation manual						
2. LMSmodular configuration guide						
3. LMSmodular configuration reference						
4. LMSmodular user guide						
5. LMSmodular Access Control Manual						
6. LMSmodular Guard Tour manual						
7. LMSmodular Graphic Station manual						
8. GW21 Technical Manual						
9. GW20 Technical Manual						
10. CMX Technical Manual						
11. CIT / DOGGY / CBS-3 Technical Manual						
12. NISE / NISE_CNF / FHI_PAD Manuals						
13. System Summary and Engineering Guideline manuals						
14. Data Sheets (GW20, GW21, CMX)						
15. Application notes: LMS News						
16. PC-Based, interactive documentation (TeachWare)						

Comments / suggestions

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