ENGIBY
Ch. des Fauvettes 3
1580 Avenches
support@engiby.ch
www.engiby.ch

Avenches, March 2018

NG Server

Functional Description

ENGIBY

Contents

1 Introduction

This document is a general functional description for a NG-Server system. The package is built in a set of modules where some can be installed or not, may run on different computers or even be installed on several computers as to ensure redundancy. Some features are optional and might be restricted unless a suitable license is delivered and activated. As far as possible, the various options, with license restrictions are described as such. Some small options are not presented but can be proposed upon request.

NG-Server is the general title used for the general concept and all components of the system. Although the concept is basically designed and optimized for Saia-PCD® systems, some features could be supported for other similar systems.

The NG-Server is firstly designed and optimized for configurations with a large number of small distributed systems (rather than individual large installations). This is achieved by mean of standardization of configuration, automatic registration of systems into the server database and dynamic adaptation of the database for each new received data table.

Typical applications realized or in test phase:

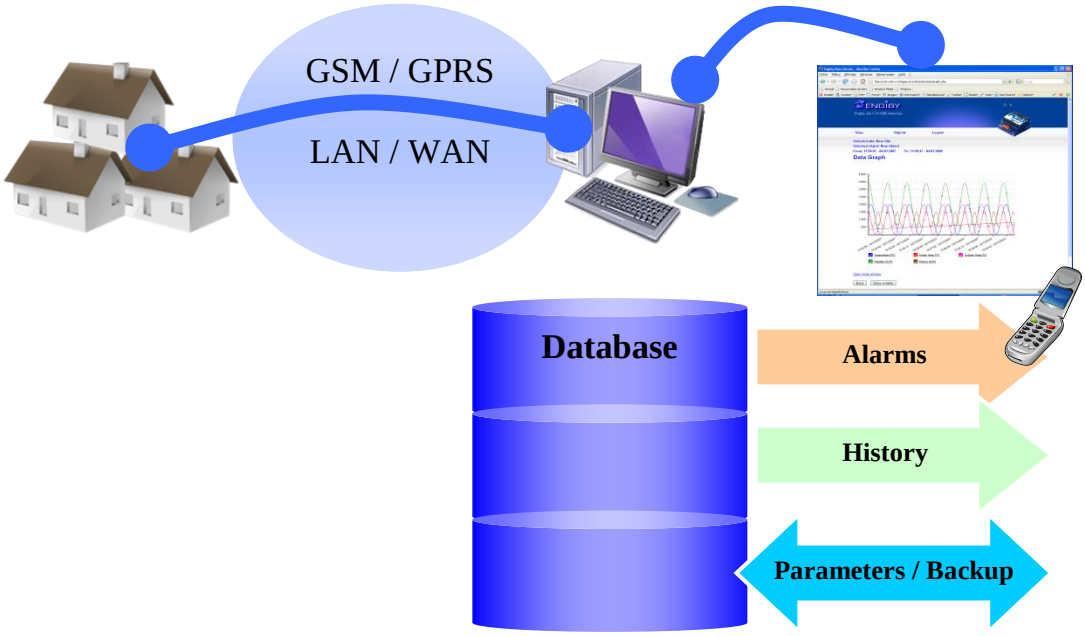
- Energy consumption measurement
- Remote maintenance of Heating plants
- Centralized alarm transmission system
- Supervision of Cooling systems
- District Heating
- Remote supervision of Pumping stations
- Remote supervision of Radio stations
- Control of public lightning

2 Basic concept

NG-Server is not a supervisor system and consequently started with a different approach. While supervisors are based on a process image principle with permanent online connections, NG-Server collects its data by packages built and sent spontaneously by the external systems. Data collection, data transmission and visualization are 3 independent asynchronous processes. As a result, the whole system has is highly tolerant against disturbances in the transmission chain from the process up to the end-user.

The main features of the NG-Server are :

a) The collection of historical data from distributed sites and the storage into a centralized database
b) The detection of alarms and simple events including transmission to the server for tracing and further processing
c) Automatic retransmission of alarms by Email and/or SMS
d) Storage of system parameters with transmission of modification in both directions
e) Values backup on SQL server and restore upon request from external systems
f) Remote survey and management of the external systems and all installed applications



Data, alarms, parameters as well as further internal auxiliary information about each system are available over a standardized web interface. The access to this data is controlled by mean of configurable access rights (user names, and passwords), site categories, object categories (for historical data), alarm categories and parameter categories. Alarms can be handled by maintenance personal over the web interface (acknowledged and archived) or automatically forwarded to predefined destinations (by the optional Alarm-Service). The connection between the external systems (Saia PCD®) and the server is based on an Intranet (LAN network) or via Internet (ADSL or GPRS modems).

3 System Features

This chapter describes in detail each part of the NG-Server concept.

- System
- Site
- History Data / Trends
- Alarms / Events
- Parameters
- Backups

Each PCD is handled as a system in the server. For a simple case, one system is bound to one site and only the site is visible to the end-user. Other relations can be configured by the manager.

3.1 System

The notion of system is reserved to the programmer and the manager of the server. The end-user will not see it.

When an external system is put into operation, it must execute a registration into the server. This will be the initial indication that a system exists and it will be added (or updated) into the NG-Server database.

Each system has a configured ID (External ID) and is registered with its serial number. Once a system is registered, no other system can use the same External ID (locked by the serial number).

All registered systems, with advanced info are visible over the web interface by a manager:

- System ID (external ID)
- System status (In operation/Testing/Demo/…)
- System name (manual entry)
- System category
- Region (to define SMS and Email destinations)
- Location (manual entry)
- System type (e.g. PCD3.M5445)
- Firmware version
- User application version
- Serial number
- IP address (local IP and public IP if present)
- Last connection date and time
- Online status (result of active connection check)

3.2 Site

A site represents a physical location for the user. (e.g. building or a production center). The end-user will firstly access to a list of available sites. The access rights for a given user are configured by the manager to a list of particular sites or a category of sites.

When a site is selected, the user will have access to its history objects and alarms. These list may however be limited by object or alarm.

3.3 Historical Data

A system will collect its data as defined by programming. Historical data are organized in objects (groups). In an object all values are recorded with the same time interval. On the server, data of the same object are display in the same table or on the same graphical representation. An object can have up to 50 values.

The values can be grouped in categories (up to 50 categories are available). For instance:
Public: Data can be viewed by the end user
Maintenance: Data can be viewed by maintenance personal
Engineer: Data can only be viewed by developers and the server manager

The data presentation (name, unit, format, color) can be standardized and all systems can present the same structure. This simplifies the organization of the server (no manual configuration of each system). It also facilitates the understanding of the web-interface and the instructions for everybody.

The data can be viewed in table or in graphical form with a free selection of the time period. Predefined selections are quickly available for 1 hour, 1 day, 1 week, 1 month and 1 year. Selected data can be downloaded locally in CSV files. CSV files can be open with spreadsheet application (e.g. MS-Excel) for further processing.

A snapshot function allows you to collect data from a group of objects for a given date. The listed data can be downloaded as CSV file. This feature is useful for comparing data from different sites at a given time or for invoicing of consumed energy

Thanks to very large storage capacity, the data can remain on the server during several years. To limit the used disk space a purge and export tool is available to the manager.

List of historical data

Example of trend data structure

Object ID	**1**
Object name	**Heating Energy counter**
Interval	30 minutes

Index	**Name / Unit**	**Grouping**	**Accu**	**Description**
0	Energy [kWh]	Last	X	
1	Volume [m3]	Last	X	
2	Power [W]	Average		
3	Volume Flow [l/h]	Average		
4	Inlet temperature [°C]	Average		
5	Outlet temperature [°C]	Average		
6	Outside temperature [°C]	Average		

Object ID	**2**
Object name	**Electricity counter**
Interval	15 minutes

Index	**Name / Unit**	**Grouping**	**Accu**	**Description**
0	Energy [kWh]	Last	X	
1	Power L1 [W]	Average		
2	Power L2 [W]	Average		
3	Power L3 [W]	Average		
4	Power total [W]	Average		
5	Voltage L1 [V]	Average		
6	Voltage L2 [V]	Average		
7	Voltage L3 [V]	Average		
8	Current L1 [A]	Average		
9	Current L2 [A]	Average		
10	Current L3 [A]	Average		

The definition of the grouping function is useful when data a grouped for representation of long period. The grouping of values will be automatically activated for large number of data but can be modified at any time by the user.

By selecting the option ‘Accu’ (Accumulator) periodical delta are automatically computed and shown. This feature is usefull for accumulated values like energies, volumes or quantities.

3.4 Alarms and Events

Alarms are detected by the PCD-System and transmitted spontaneously to the server. Upon reception, the server will update 2 tables: an **Alarm list** including all currently active alarms with the time of the last occurrence and an **Alarm history** with all occurrences of each alarm.

Alarms can be repeated by the PCD system if the alarm condition remains longer that a defined time.

Events work in the same way as alarms. The difference is on the user interface. Events will not be present in the Alarm List and event occurrences are inserted into the Event History.

Two types of alarm/events are available:

- Binary alarms/events are detected by a digital input or an internal logical condition.
- Level alarms/events are detected by a value exceeding a defined limit during a defined time.

With level alarms, the actual value, the limit and the delay are also transmitted with the alarm message.

Alarms are organized in categories and priorities.
The category allows you to define a destination for the automatic email transmission of alarms (50 categories are available).
The priority defines the urgency for the automatic transmission of alarms (10 priorities are available).

Alarms and Events are identified by a double numeric ID, called Group and Index.
A typical alarm number is then 12 / 34.

The alarm texts are stored on server side. All systems can use the same alarm texts. This simplifies the maintenance and the understanding of the alarm signals. Simpler installations may support only a subset of the alarm list. If required, the alarm text of each system can be defined differently.

The Alarm list and the History list on the server allow you a precise tracking of alarm with the following time stamped events:

- detection of alarm condition in the PCD
- end of alarm conditions in the PCD
- reception of the alarm in the server
- acknowledgement over the Web interface
- deleting of alarm over the Web interface
- automatic transmission of the alarm by Email or SMS

Alarms can be acknowledged over the Web interface. Acknowledged alarms are marked with a particular color. Optionally, Acknowledged and Reset alarms are automatically removed from the alarm list.

Thanks to very large storage capacity, the alarm history can remain on the server during several years.

The alarm transmission service is described later in this document.

ENGIBY

List of alarm signals
Example of alarm texts and properties.

Alarm Group	**1**			
Default Category	**2 = Heating**			
Default Priority	**2**			
Alarm	**Text**	**Language 1,2,3**	**Priority**	**Category**
1 / 0	General heating fault		Default	Default
1 / 1	Low temperature		Default	Default
1 / 2	High temperature		Default	Default
1 / 4	Pump fault		Default	Default
1 / 5	Pressure High		1	1
1 / 6	Pressure Low		1	1
1 / 7				

Alarms can have 3 optional texts for 3 different languages. Language texts can be used for automatic sending per Email or SMS.
Default Category and Priority are defined for each group in the PCD system. For each alarm, the Priority and the Category can be overwritten on server site.

Category list
Example

Category	Name	Description
1	System	PCD System errors. E.g. Low battery, IO-failure, Bus Extension failure
2	Heating	
3	Cooling	
4	Lighting	
		To be completed
50		

Priority list
Example

Priority	Name	Period 1 Start	Period 1 End	Period 2 Start	Period 3 End
1	Urgent	00:00	23:59		
2	Middle urgent	06:30	18:30		
3	Non-urgent	08:00	12:00	13:30	18:00
4					
5					
6					
7					
8					
9					
10					

3.5 Parameters

The parameter function needs the installation of the optional module TCP-Transmitter with a suitable license.

A system has a number of parameters grouped in parameter tables. Parameters can be binary status, numeric values (e.g. set points) date or time for clock functions.

When a parameter is changed in the PCD (by an automatic adaptation or manually) the new value is sent to the server. At any time, the last stored parameters can be restored into the PCD by mean of a request to the server. This ensures an optimal continuation of the operation in case a PCD must be exchanged or when data have been cleared.

3.6 Values Backup

The Backup function needs the installation of the optional module TCP-Transmitter with a suitable license.

The backup mechanism is similar to the parameter. Values can be sent from the PCD and will be stored in the SQL database. At startup or upon request, the values are restored back into the PCD.

However, backup values are not visible over the user interface and cannot be edited over the Web interface.

This feature is useful for system running without battery or to restore local values when a system must be exchanged.

4 Server modules

The server is split into several applications or services. This allows the distribution of the function over several PCs, at different locations, and to duplicate some processes for better performances or redundancies.

For customized applications standard modules can be combined with specific ones to fulfill a particular specification.

4.1 TCP-Receiver

This service is in charge of the reception of data packages from the PCD systems over TCP ports. It is always listening on the configured TCP port. Two ports are open for TCP connections, a low priority and a high priority port.

The low priority port is used to receive big data packages (historical data). It can be busy for long time.

The high priority port is used for alarms reception and other short transactions like registration and IP address updates. These functions are ensured even during transmission of large data packages.

Optionally, the TCP-Receiver can set the PCD clock each time a connection is established.

For very large applications, with a suitable license, up to 200 ports (100 low + 100 high priority connections) can be supported simultaneously. This may be required on large applications or with GPRS modems where the transmissions may take long time.

With a suitable license the TCP-Receiver can duplicate the received data package, for instance on 2 disks as to realized a database redundancy.

4.2 TCP-Transmitter

This module is in charge of the transmission of parameter and backup values from the server over TCP ports toward the systems. It regularly scans the parameter tables in the database. When tables are marked for transmission, it automatically calls the external system and sent its parameters.

An Online check function can be activated to regularly poll each system and update its online status into the database. This status will also speed up the transmission process when a large number of systems must be updated at the same time. Offline systems will be skipped until the online check succeeds again.

Optionally, the TCP-Transmitter can set the PCD clock each time a connection is established.

4.3 DB-Loader

The DB-Loader service is in charge of decoding the received data packages and loading into the database. Data packages are passed by temporary files received by the TCP-Receiver.

With a suitable license, data can be collected from 2 remote locations (logical disks) allowing the realization of a redundant system. This feature is necessary when one or 2 instances of the TCP-Receiver run on other PCs.

The DB-Loader service is also in charge of checking the systems configured for life check. If a system has not established a connection within the maximum specified delay, an alarm is created.

4.4 Web server

The web server is based on standard web applications:

- MySQL data base
- Apache web server
- PHP interpreter

Licenses for these applications are not part of the Engiby delivery. The standard web pages however, installed on the web server are provided by Engiby. This package allows you an immediate access to the stored data, the alarms and parameters. All texts of the user interface are delivered in English, German and French. One more language is available for free translation. Each user can choose its own language.

The web interface is described more in detail later in this document.

4.5 Alarms Transmission

The alarm-Service needs to be installed and activated by a suitable license. Depending on the license, one or 2 Email server and 1 or 2 SMS server are supported. In case of failure of an Email or an SMS server, the 2nd one is automatically used.

Failure of Email servers can be reported by SMS while failure of SMS servers can be reported by Emails.

With the optional Alarm-Service, alarms are automatically transmitted to predefined destinations (Email and/or SMS) according to the priority. For instance: Urgent alarms are transmitted during day and nights, non-urgent ones are sent during working days and working hours only. The server also supports a permanent calendar allowing the delay of alarms during bank holidays.

The alarm transmissions are configured by mean of Transmit conditions. Each transmit condition is allocated to a site category.

The available transmission types are:

- Global — For all alarms of the site category
- Site — For all alarms of one site
- Category — For all alarms of a category
- Priority — For all alarms of a priority
- Site/Alarm — For one particular alarm of one site

For each transmission condition, the destinations can be defined:

- Directly in the condition
- By a parameter of the site (for compatibility with former configurations)
- By a destination group (for management of destination over groups)
- By a user name (for management by the user itself)

Each destination can include up to 10 addresses (SMS or Email).

The email and SMS format is defined by templates stored in the data base. A different template can be used for each transmission condition. Default templates are delivered with the package and can be adapted as required.

The transmission of SMS needs an SMS account with Internet access using an API. Because each provider supports its specific method, the implantation of the API must be first agreed with Engiby.

5 Web User Interface

A standard HTML5 Web package is part of the NG-Server concept. The end user will have access to the stored values and alarms. Each user has its own user name and password which tailors its access rights.

For the trend data view, the user has a selection tool for the site, the object (data table), the values and the time period. The selected data can be viewed in tabular or graphical form and downloaded as picture or CSV file.

The alarms can be viewed in a list of actual alarms with possibility to acknowledge and remove alarms. A historical list of all alarms allows the precise tracking of alarm events (alarm detection, reception, acknowledgement, transmission and removal).

A special manager account automatically has access to all values and alarms on the user interface.

6 Web Manager Interface

The HTML5 Manger Web interface offers the possibility to configure and manage all systems, define sites, objects, value names, alarm texts and users.

The manager has also a number of internal tables to control de functioning of the server:

- Sever events (User Login/Logout, application Start/Stop)
- Server errors
- System events (Power Off/On of PCD-Systems)
- Receptions (statistic of quantity and frequency of received data)

7 Security and reliability

As soon as systems and data are available over Internet, the notion of security is a topic of discussion. In this chapter, we also consider the aspect of reliability of the data acquisition and transmission. Finally the system must be secure against unwanted accesses but also offer an intrinsic security and reliability against disturbances of the used infrastructure.

The reliability and availability of the system has also been considered as an important aspect of the NG-Server concept. The main features are also described in this chapter.

For the analysis of the security, we must consider that the foreseen uses of NG-Server are not critical applications. If however, critical situations may be the consequence of the use of the NG-Server, the security aspect must be specifically discussed with Engiby in advance. In any case the appliance of the appropriate security is under the responsibility of the user of the finale solution. Engiby cannot be liable for the use, missus or lake of uses of the server or the stored data.

7.1 Web access

Two cases must be considered.
1) In case of an Intranet application the access of the web server can be restricted for internal uses and the Internet attack can be avoided (or covered by the general Intranet access security).
2) In case of a public access the web server must be published and is available for anybody from anywhere on Internet.

As long as information is only displayed, the external attack doesn't have much consequence. The most critical part is the parameter pages. If not really used, this feature can be totally disabled.

Name and Password: Each access is protected by mean of user name and password. The passwords are encrypted before to be stored in the database.
Two different encryption methods are available: Password V2 and V3.

Passwords V2 have an MD5 encryption which is not very strong especially with short passwords.

Passwords V3 are strongly encrypted and even an access to the database does not permit the decoding of passwords. This method should not be used if the security or confidentiality is an important topic.

When a user log in, the access with the higher version is attempt first, and the lower if not granted. After a successful login, the used password version is shown to the user.

Login Timeout: A logged user without activity is rejected after a definable timeout.

SQL Injections: The risk of SQL injection has been considered and is avoided.

Brute force: This is the simplest attack to attempt. It generates systematic attempts sent to the server to find a valid login name and password. This is avoided by delaying new login after a number of failing attempts (e.g 15 min delay after 5 falling attempts) and a definitive locking of a user after a larger number of attempts (e.g. after 100 failing attempts).

7.2 Database connections

To limit the possible attack from Internet, the access to the data base is not open for Internet access (must be configured when the database is installed). The web server is normally installed on the same PC as the database and only access from the local PC is allowed. This security is also under the responsibility of the customer since the MySQL database is not part of the Engiby's delivery.

7.3 Parameter editions

The access to parameter tables and individual parameter can be restricted to the concerned users by mean of parameter category.

Each modifiable parameter has minimum and maximum limits to avoid the unwanted and erroneous adjustment of dangerous values.

If required, further check and security must be added in the PCD program itself.

7.4 Systems mix-up.

Due to the fact that external systems are put into operation at different time and by different people, geographically distant, the risk of mix-up of data from different systems is quite high. This risk is drastically reduced by the use of serial numbers. A registered system is identified in the database with a unique ID (defined by the manager) but also locked with its unique serial number. No data from other systems (different serial number) are accepted under the same system ID.

7.5 Alarm transmission

The same server is used to slowly transmit large data packages as well as quick small alarm signals. The concurrent use of the same server with a large number of systems has been considered. In case of alarm, the PCD use a high priority port, while large data package use the low priority port. Even during transmission of large packages by several systems, another system can immediately send alarms over the other port.

7.6 Redundant server

For large applications, it may be important that data transmission is always ensured, even when the server is shut down for maintenance or the connection is not possible because of a defective element (server or network). To cover this case a redundant system can be built. The PCD will have 2 server connections and will automatically try both alternatively.

This does however not solve the case of problems on PCD side.

7.7 Data confidentiality and manipulation

In some cases, one would not want that exchanged data are visible and readable over Internet. Because the intended applications are not critical, no particular encryption is used so fare. However, the exchanged data are not plain text but mainly binary coded and have no clear meaning without deep knowledge of the used codes and structures. For the same reason, data manipulation is almost impossible. Data package that are not correctly structured will be rejected before storing in the database.
These remarks are only valid for data exchanged between PCD and the server but not for the Web access as well as for alarms transmitted per email or SMS.

7.8 Transmission disturbances

Transmission disturbances can avoid the transmission of data packages. The establishment of communication and the data exchanges are protected by checksums and timeouts. If a package is not completely and correctly transmitted, it will not be acknowledged by the reception application and resent by the PCD.

If no correct communication is possible during a long period, the data remains stored in the PCD memory. The PCD autonomy can be estimated and adjusted specifically for each application.

If such situations are likely to occur frequently an optional function can be added in the PCD allowing to copy the stored data on a removable flash and free the buffer memory. Such data can be manually re-injected on the server.

7.9 Online check

To ensure that a system is always available (e.g. for sending of parameters), an online check mechanism is implemented. The regular active checking of the availability of the systems ensures that connection breaks are detected before a connection to the system is effectively needed.

7.10 Life check

The life check is a passive mechanism useful even if connection toward the external systems is not possible or not wanted (GPRS or ADSL restrictions). A survey of the connections interval for the data delivery from the PCD toward the server is checked. A missing connection within a defined maximal period indicates a problem of the external system (system out of order or broken network connection).

8 Network configurations

The NG-Server work best with direct LAN connections. The following variants are described here:

- Intranet
- Internet over (A)DSL
- Internet over GPRS

Further configuration can be supported after discussion with Engiby.

8.1 Intranet

With Intranet it is assumed that all PCD systems as well as the NG-Server PC are on the same internal LAN network. All PCD systems and the server have a fix IP address.
This is the simplest case and no particular configuration is required.

8.2 Internet over ADSL

This applies to a structure where the server is accessible over Internet and the PCD systems are distributed on external sites with an (A)DSL connection. The (A)DSL router generally gets a dynamic IP address. The server however must have a fix public address. In this way, the PCD can contact the server at any time. If required, connect requests from the server toward the PCD (parameter and online check) must be routed by a specific configuration in the ADSL router (ports 5082). A special feature ensures a regular update of the dynamic IP address of the (A)DSL router into the server database. In this way, the server has always (or within a known delay) the correct IP address to contact the PCD system.

Operation without update of dynamic IP address is possible by excluding any transmission from the server toward the PCD systems. Only registration (without confirmation), data storage and alarming are then supported.

8.3 Internet over GPRS

Depending on the contract with the GPRS network provider, these cases must be considered.

1) Contracts with fix IP address are similar to the Intranet case described above.

2) Contracts with dynamic public IP address are similar to the (A)DSL case described above. However, the IP address can be checked locally and the server must only be contacted when this address changes.

3) Contracts with dynamic private IP addresses which cannot be reached from the internet (which is the usual case of a contract, e.g. for a smartphone). In this case the PCD can connect the server for data and alarm transmission, but any transmission from the server to the PCD is not supported.

9 Requirements

Those are some particular requirements for the PC running NG-Server applications and the network configuration.

9.1 PC requirement

NG-Server modules are designed and tested to run on 64-bit versions of

- Windows7
- Windows 10
- Windows Server 2003
- Windows Server 2008 (R2).
- Windows Server 2012

The TCP-Transmitter application does not run as service and therefore an auto-logon user must be configured. A link must be created in the auto-start menu to start the modules at each startup of the PC.

A MySQL database and an Apache Web server with PHP interpreter must be installed. The open source package Wamp Server 2 can be used for this installation. No licenses nor support contract are included in the Engiby delivery for this part.

For a more secure access, HTTPS can be configured on the server. This task is not part of the Wamp Server setup and also not part of the standard Engiby's delivery. It can be realized by Engiby on request.

Public Internet Providers are generally not suitable because Windows applications cannot be started and direct SQL access are not allowed. If you cannot use your own PC, you should rather find provider where you can rent a virtual PC with Windows operating system. If required, this task can also be ensured by Engiby.

Due to the fact that the TCP-Receiver is passing the received data in the form of files to the DB-Loader, the disks of the servers running the TCP-Receiver and the DB-Loader need to be defragmented in a regular interval.

For a medium-sized NG-Server installation (~200'000 recorded values per day for one year → ~2GB/year) the following specifications should be fulfilled:

- 4-8 GB RAM
- 100 GB Memory (HDD, not SSD), to be checked after few months of operation whether the estimated 1 year data will require more space
- 2.5 GByte dual-core CPU
- Windows server 2008 R or newer, 64-Bits

9.2 Network requirements

To allow the communication from all PCD toward the server the following ports must be open and routed to the server:

- 5080 = Low priority packages
- 5081 = High priority packages

The server PC must have a fix IP address or must by accessible from outside (Internet) with a fix public address.

To allow the communication from the server toward all PCD, the following ports must be open for outgoing connections:

- 5082 = For all connections

To allow the access to the Web server for anybody from Internet, the HTTP port (default = 80) must be open and routed to the server. If used, the same must be done for the HTTPS port (default = 443).

A monitor application will be installed to monitor the installed services. This tool will use several TCP ports in range 5083 to 5089. If it is necessary to monitor the services from another PC on the network, these ports must be open and routed to the server.

The ports mentioned here are only default settings. Other port numbers can be used if required but must also be adjusted on the external systems (PCDs).

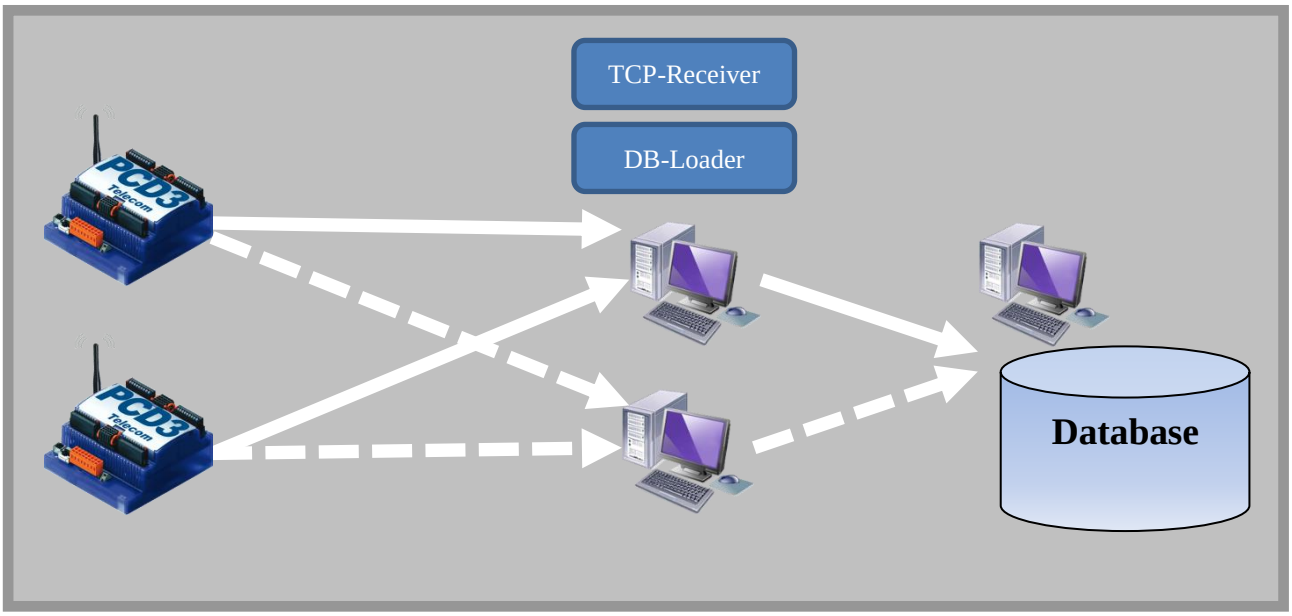
10 Redundancy

Two typical concepts of redundancy can be realized:

- Communication redundancy
- Data base redundancy

10.1 Redundant data reception

To realize a redundancy of the communication over the LAN, the PCD is configured with 2 IP address. Over the LAN, each of them can have a different route to reach the server.
On server side, 2 computers, running a TCP-Receiver and a DB-Loader are present. Behind those, one server running the SQL-Database is located. The DB-Loader writes the data over the MySQL connection to the server.

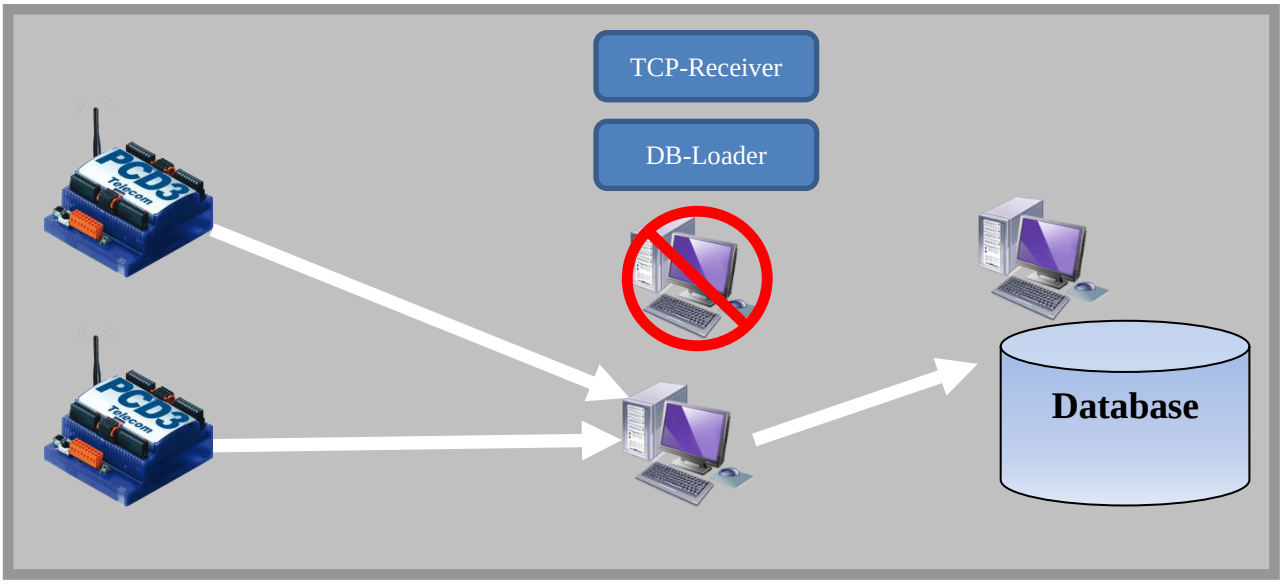


In this constellation the Alarm transmission can either be realized on the Database server or on an additional machine beside the Database server.

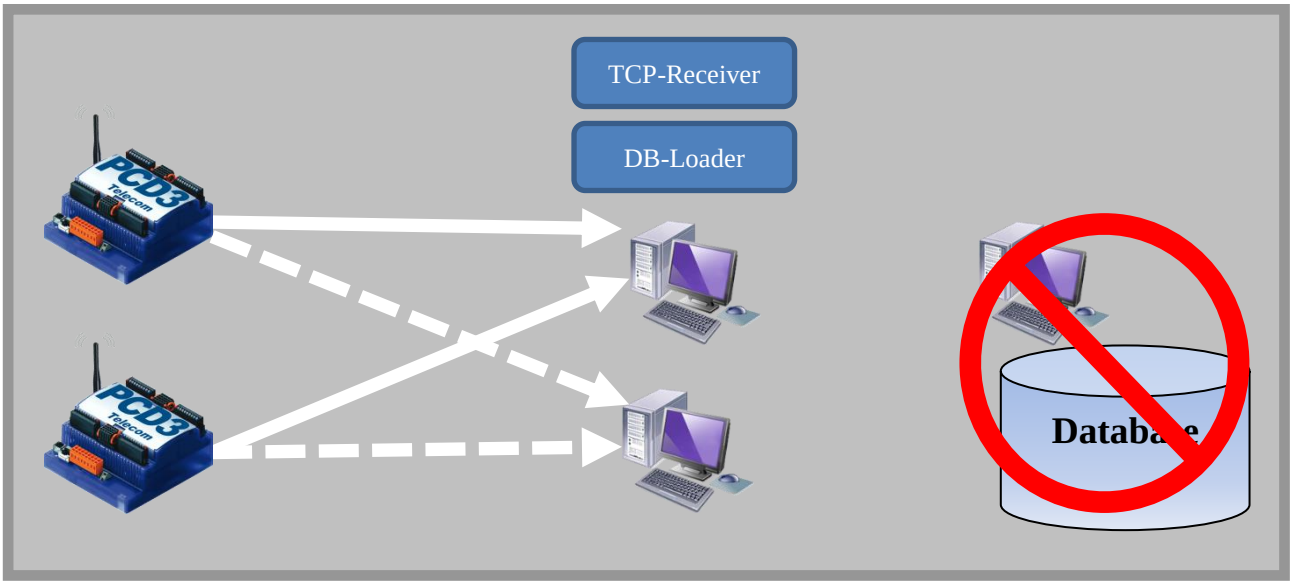
To avoid a loss of the data stored in the database the following possibilities exist:

- A regular dump could be executed (e.g. once a day).
  Note that in this constellation in case of a DB failure data since the last dump are lost.
- The database could be run in a master-slave constellation.
  This constellation allows the 'live access' to the slave database, e.g. for web access.

Functioning in case of one communication PC failure
In case one of the PCs which run the TCP-Receiver and the DB-Loader fails (or the network connection from the PCDs to this machine), the PCD will connect to the second configured TCP-Receiver. From this machine the data is written to the same database by the DB-Loader on this machine



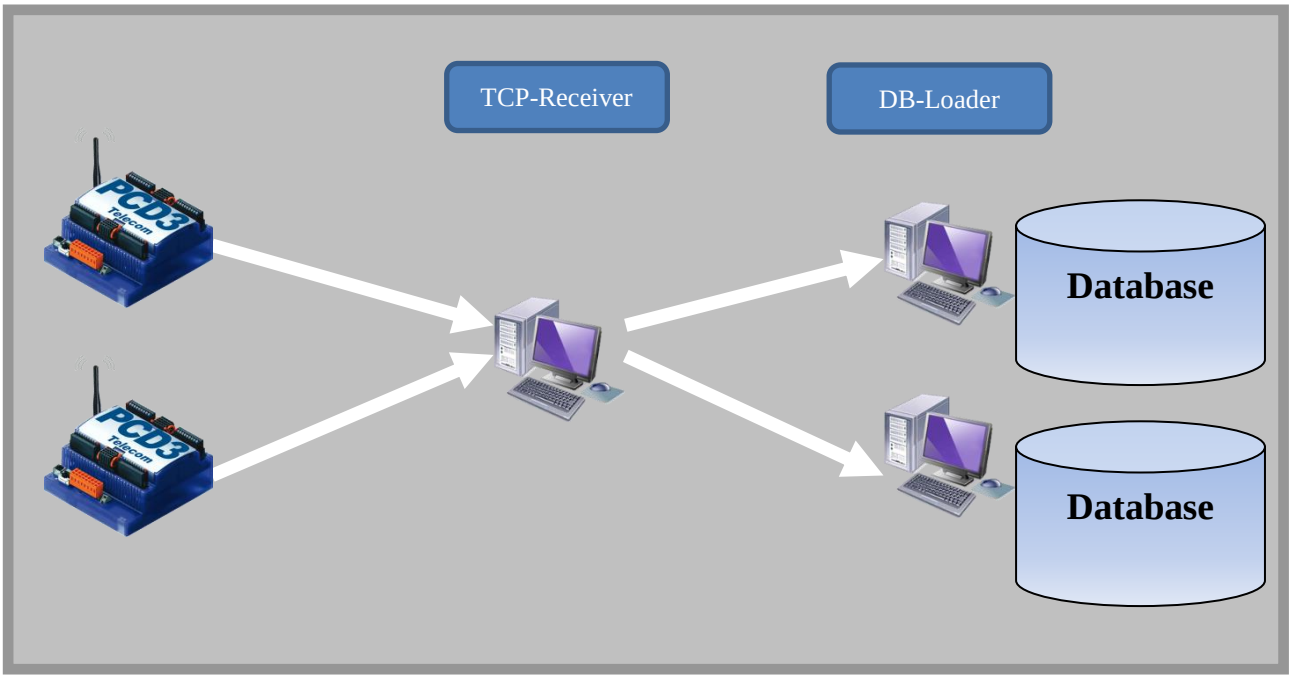
Functioning in case of DB failure
In case the Database server fails, the DB-Loader will stop due to the missing SQL connection. The TCP-Receiver will continue to run for the time specified in the license (up to 4 days) and store the received data to temporary files on the local drive.
Once the Database is running again, the DB-Loaders will continue to run and store the data from the temporary files to the database.



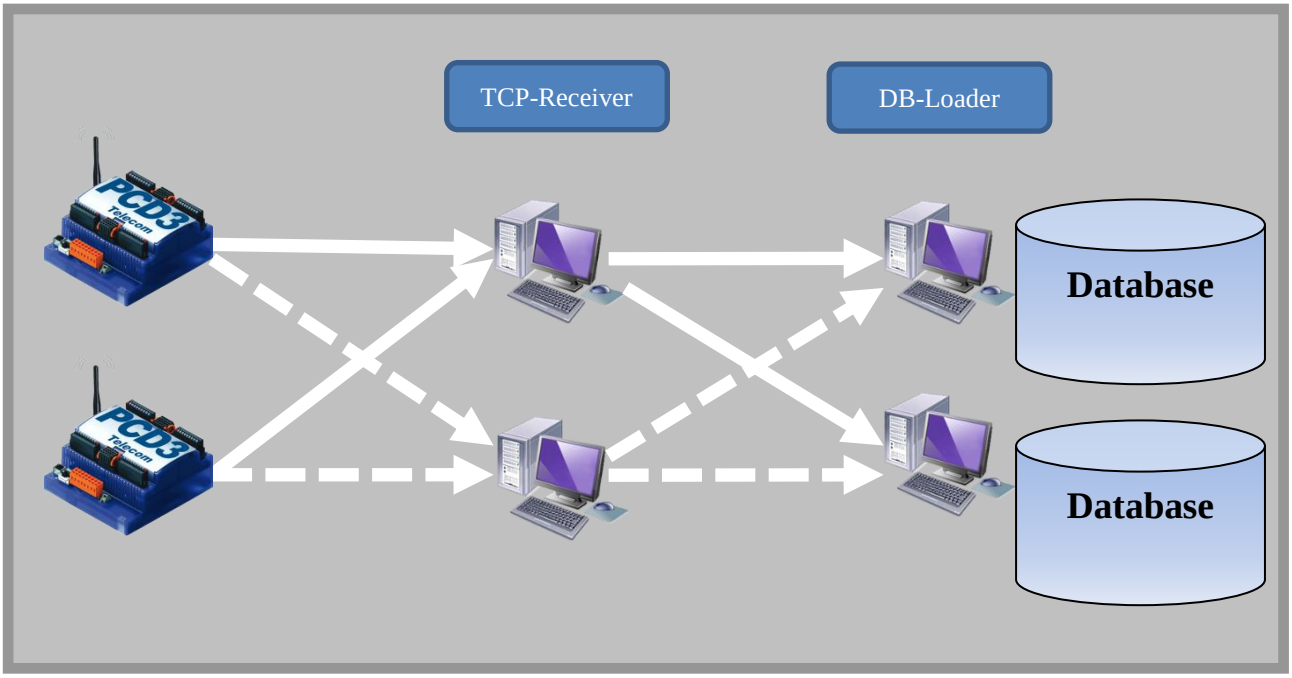
10.2 Redundant databases

A redundancy of the database can be realized by setting up 2 DB-Loader and 2 Databases on 2 different computers. The TCP-Receiver will be configured to duplicate the received packages.

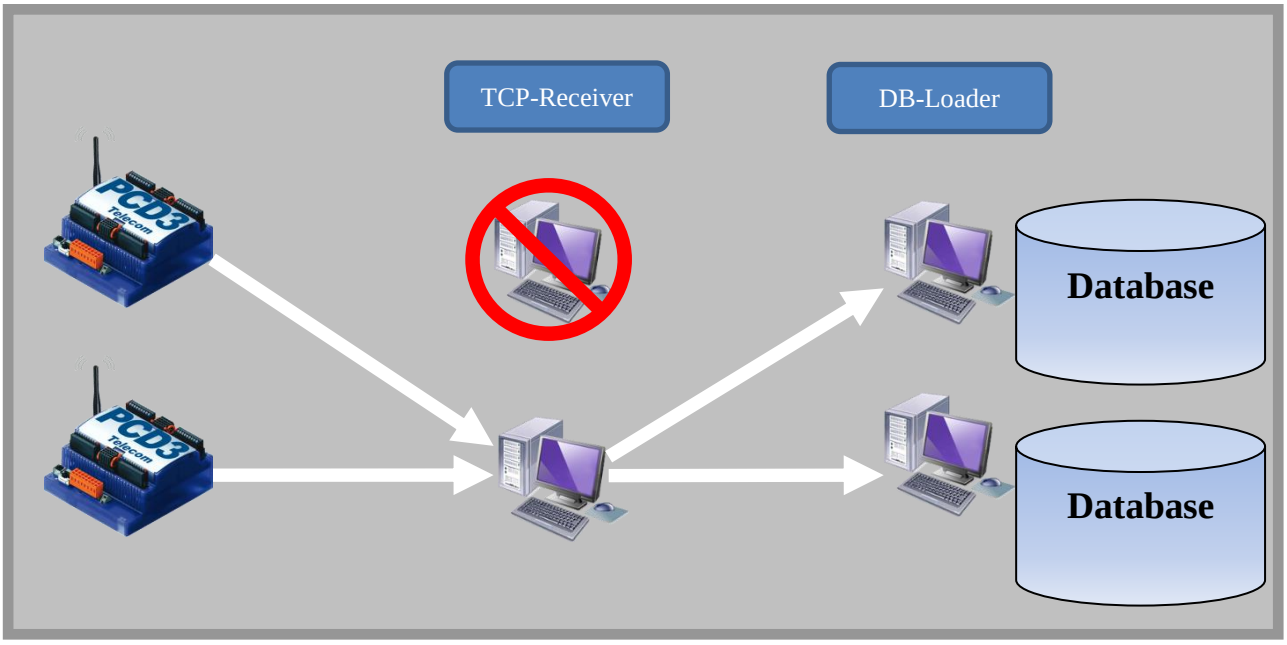
In case of missing data on one database (failure of DB-Loader computer), the data can be found on the other one.



A full redundancy of the communication and the database can also be realized by combining the 2 diagrams.



Functioning in case of Receiver failure



11 Limitations

The NG-Server can be used in many different cases and this chapter intends to provide information about the optimal design of large installations.

As general role the limit of the system is at **1000 systems**.
However, as the limiting factor to the NG-Server is the amount of data stored over a certain time, this number must be reduced according to the recoding interval, the number of objects and values per object.

Based on existing installations and our internal calculations and test it was found that a total of **10 Mio stored values per day** should not be exceeded in order to obtain well working NG-Server installation.

The calculation formula is given below.

The purchased license also set some system limits as described in chapter below.

11.1 Computing of maximum amount of systems

The following formula can be used to calculate the maximum number of systems which can be connected to one NG-Server:

$$n_{systems} = \frac{10'000'000 * t_{interval}}{1440 * n_{obj/system} * n_{vals/object}}$$

$t_{interval}$	Value recording intervals in minutes
$n_{systems}$	Number of connected systems
$n_{obj/system}$	Number of object per system
$n_{val/object}$	Number of values per object

Derived cases:

- ➔ **15 minutes record interval**
  10 objects with 10 values per system
  → 1041 Systems -> License limit = **1000 systems**

- ➔ **5 minute record interval**
  5 objects with 10 values per system
  → 694 systems

- ➔ **1 minute record interval**
  3 objects with 5 values
  → 462 systems

11.2 Limits set by license

The highest limit that can be set by the license is:

- 1’000 systems
- 10’000 objects

Other licenses reduced the number of systems to 128, 64, 32, 16 or 8.
The maximum number of objects is always 10 times number of systems.

The maximum number of alarms is only given by the alarm numbering which is 65’536 groups with 65’536 indexes.

Number of simultaneous TCP connections: 100.
The basic license limits it set to 1 connection.

Number of redundant TCP-Receiver: 2
Each TCP-Receiver needs its own license.

Nicolas Bovigny / Christian Durrer / Engiby sàrl