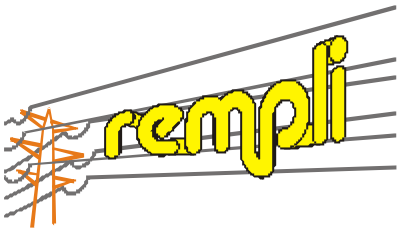


# REMPLI

***NNE5–2001–825***

***Real-time Energy Management via Powerlines and Internet***

White Paper

# REMPLI Security Concept Overview

| | |
|---|---|
| **Document type** | White Paper |
| **Document version** | Final |
| **Document Preparation Date** | |
| **Work Package** | WP 1 / System Specification |
| **Task** | T 5 / Security Strategy |
| **Classification** | Restricted |
| **Contract Start Date** | 01. 03. 2003 |
| **Duration** | 36 months |

**Project funded by the European Community under the "Energy, Environment and Sustainable Development" Programme (1998-2002)**

# Contents



 

# 1 Introduction

This document gives an overview of the security strategy used within the REMPLI system – a communication system used for meter reading and SCADA tasks. REMPLI uses an IP-based private network (REMPLI Intranet) and the public powerline network (PLC). Since the used networks, especially PLC, are publicly accessible and therefore must be regarded intrinsically as not trusted, communication from and to the Node, connecting the meter or SCADA (Supervisory Control And Data Acquisition) equipment to the network, must be protected. Fig. 1.1 shows the security relevant components of the REMLI system.

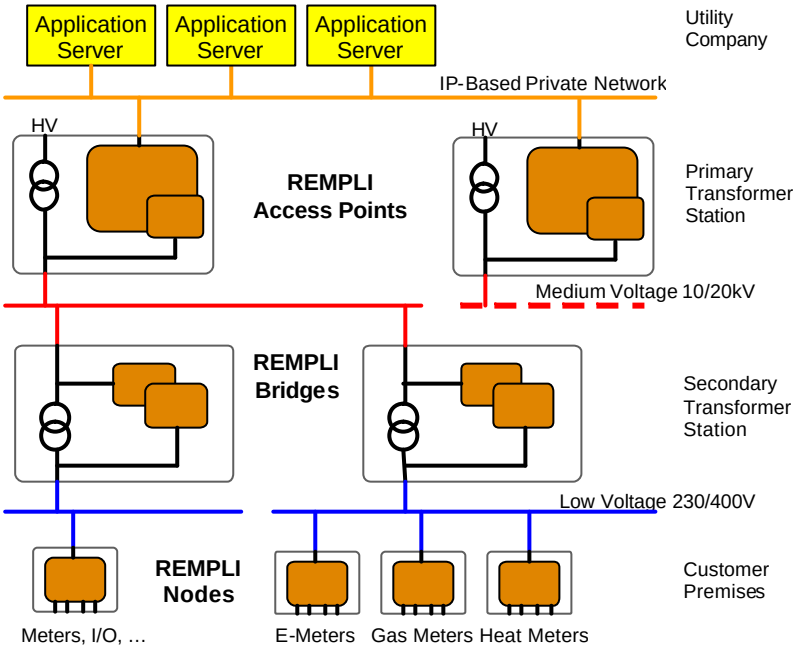


Fig. 1.1 General system overview of the REMPLI system

The REMPLI system, like other telecommunication systems that are used for meter reading and SCADA tasks, must carefully handle transmitted data to avoid manipulation, information theft or even physical damage and human casualties due to manipulated or distorted data. These requirements demand security services to quarantee confidentiality, intergrity and authentication of data, although the focus is primary shifted to authentication and integrity (also refer to SELMA - Project for secure electronic metering data interchange, www.selma-project.de, for more information).

Unlike (public) telecommunication systems used for meter reading and SCADA, which use point-to-point and high bandwidth connections, the REMPLI system has two special aspects to consider:

1. The PLC system, used by REMPLI, is a shared medium with very restricted data transmission capacity that can be accessed by everyone. Therefore, security protocols and measures must be carefully designed and optimised to fit into the limitations of the (powerline) communication system (PLC): to low-bandwidth, packet oriented, and stateless data. Security measures used in existing systems like telephone call-back or simple password protection are not sufficient to protect the REMPLI system.
2. REMPLI uses a combination of an IP based medium-to-high bandwidth private network (REMPLI Intranet) and the PLC. The Access Point is the connecting element between these two worlds, which have different capabilities and security needs.

This document will start with presenting the hazard and risk analysis, then introducing the security concept, and finally discussing integration of the REMPLI security policy and a utility's security policy.

 

# 2 Hazard and Risk Analysis

The goal of the REMPLI project is to define a communication system to allow for remote meter reading and transmission of SCADA messages over a PLC and a private IP-based network. Since REMPLI system should also be open for additional future usages, the data (format) is not limited to metering and SCADA information; instead, we have to assume generic, packet oriented "unstructured" information. Nonetheless, the main focus within the current security strategy will be made on

1. Metering data and
2. SCADA data

according to the standards IEC 60870, IEC 62056 (also known as IEC 1107) and M-Bus.

## 2.1 Involved Entities

The entities involved in the process of running the REMPLI system are

1. Service provider (utility company);
2. REMPLI system operator and maintenance personal;
3. Customers of the service provider (users of the service) – Customers that are private as well as industrial consumers of the service;
4. Unknown third parties.

The process of designing the REMPLI system is intentionally excluded from the security strategy solely because REMPLI is not intended as a high-level security system. Hence, it is assumed that developers are trusted not to deliberately include security flaws or other backdoors.

The intentions of entities are hard to define, since they may vary regionally, depend on social background and many other parameters. Even within the field test in REMPLI there are groups of entities with big differences. Assumptions taken in this section are based on experience only and therefore can just give worst-case estimations.

Customers can be divided into two groups: small private customers and industrial customers. Seen as a security threat, intention of the customers would be to manipulate the system to save money by consuming energy without paying. Technical knowledge will be in general not sufficient to manipulate the system directly. These entities will either involve unknown third parties that supply equipment to circumvent the security measures of the system or simply bribe personal of the service provider or system operator to install a supply for "free" energy.

Service providers will most likely have a small potential for malicious activities. This assumption is based on the following facts:

- The intention of service providers is to control their customers and prevent misuse;
- In most countries billing-relevant data must additionally be stored in a device at customers premises, which must be certified as "tamper-proof";
- The service provider wants to provide a stable service;
- For today's systems, service provider is also a system operator.

The system operators must be a trusted third party for the former two groups by definition because they run the communication service and install the system. Hence, they are also able to manipulate the system and transmitted data, except if service providers implement additional security measures on top of REMPLI,

 

which is not assumed in this document. For practical reasons this assumption will not be completely correct and access to security-relevant components (e.g., keys) should be restricted to a small group only. This will also rule out a scenario of customers bribing (low-level) maintenance personal.

Unknown third parties are, most likely, the most dangerous. Whereas manipulation of consumed energy is not rated as a high risk by service providers, two important scenarios must be associated with attackers that are non-system participants:

- Acts of vandalism and sabotage: especially if SCADA systems that control the distribution grid use REMPLI communication infrastructure, whole distributions grids can be disabled.
- Development of devices that enable customers to forge their energy consumption: Strict legislation and detection mechanisms at SCADA level are countermeasures. Project partners assume that in Western Europe this scenario is negligible.

## 2.2 Values to be Protected

Four general classes of protection can be identified in the REMPLI system:

1. Availability of data – meaning that data is on hand when needed;
2. Integrity of data – meaning that data cannot be manipulated;
3. Authenticity of data – guaranteeing that data is sent by a particular entity;
4. Confidentiality of data – allowing only authorized entities to access data.

Due to the fact, that values to protect cannot easily be classified in absolute terms like monetary loss or probability of occurrence, the above classes are usually divided into several subclasses. E.g., confidential data can be sub-classified into confidential, secret, and top secret. In REMPLI the following security subclasses will be used to classify the importance:

1. not needed (no security measures needed);
2. low;
3. medium;
4. high.
5. very high

### 2.2.1 Equipment

Equipment is the hardware of the REMPLI system including Nodes, Access Points, metering / SCADA hardware and communication interfaces.

Concerning the equipment, availability and integrity are the values to be protected to guarantee correct functionality. No changes may be done without proper authentication of the person to change it. Measures range from having a physical key to access the equipment to username/password login and even cryptographic authentication. It is also vital that loss of one system component does not jeopardise security of the system.

### 2.2.2 Data Transport

The usual way of transporting data is a packet-oriented request/response mode, where the Application server asks for a certain value and metering / SCADA equipment delivers it. Additionally, Nodes can independently raise alarms. Node-to-Node communication is not planned within the REMPLI system.

The most important value of a communication network is its availability. Powerline communication availability is hard to guarantee, because everyone has access to the powerline even within his/her private property. It is easy to install broadband disturbers, circumvent equipment via short cuts or disconnect a Node from the powerline. The situation is just slightly different for the REMPLI Intranet. In the worst case, this

network is also a publicly accessible media (e.g. air cabling) and its availability could be tampered. Additionally, if REMPLI Intranet is a public network, denial-of-service attacks and intrusion attempts have to be considered.

Availability cannot be protected actively. The only measure to be taken inside the REMPLI system is to detect, that components are not available. This knowledge is used to enable countermeasures (within or even outside the functionality of REMPLI) to track down attackers and to narrow the affected segments (e.g. low-voltage branch, …). Since even in normal operation Nodes, Bridges and Access Points might be disconnected from the network, these devices must be able to stay offline at least for up to 30 days without loosing any data.

### 2.2.3 Metering Data

One of the main goals within the REMPLI project is to set up an infrastructure for automated meter reading. Metering data can consist of single metering data point or a complete data set (e.g. daily log). Metering data is unidirectional: it is produced only at the Node and delivered via Access Point to an application at the utility company. Metering data is transmitted only in request/response mode.

Beside general requirements to data transport, integrity of metering data is the most important value to be protected. In addition, if metering data is used for billing purposes, it must not be altered during transportation in order to retain the integrity of certified metering equipment (PTB auditing).

| Value to be protected | Security level (Priority) |
|---|---|
| availability | high |
| integrity | high |
| authenticity | medium-high |
| confidentiality | low |
| non-repudiation | low-medium |

Table 2.1 Security level of metering and SCADA tasks in REMPLI

Non-repudiation is not of a high priority, if only the total power consumption is measured. For load-dependent tariffs and load profiles, where history of measured values is important, its priority will be higher. Nonetheless, according to other research projects (e. g., SELMA project) this will at least be a medium term goal. Hence, for REMPLI the security level is ranked low to medium.

### 2.2.4 SCADA Messages

SCADA data is used for remote control and supervision purposes. Possible applications can range from control of network infrastructure (e.g. switches in transformer stations) via cutting off or turning on relevant services for customers to remote control of the customers own equipment. Due to the fact that such operations can heavily affect power supply or control and SCADA equipment of customers, it is vital that authenticity of messages can be verified securely and messages are not manipulated.

If network operator, service provider and customer do not belong to an identical organizational unit, non-repudiation and self-contained communication channels are important issues. In case infrastructure is leased to different service providers, the above values have to be ranked high.

## 2.3 Hazards and Risks

Security is always a trade-off between security, costs and convenience. To find a balance between these three objectives, hazards and risks have to be analysed and the threat should be quantified to allow an “optimal” usage of resources.

Prior investigations and answers to the REMPLI questionnaire revealed, that at the moment there is little concern about security. The general opinion, also reported by project partners, is that manipulation can be

detected by Application Servers, which are in operation today. Besides, in Western European countries legislative hindrances are so strong, that in reality fraud in metering applications can be almost neglected.

Hazards and risks can be classified into two groups: metering applications and SCADA applications. They can also be further sub-classified into

- direct manipulations of input and output values,
- manipulation or replacement of equipmen,t
- manipulation and insertion of data in the PLC network,
- manipulation and insertion of data in the REMPLI Intranet,
- manipulation at the Application Server,
- denial of service.

The considerations and investigations have been based on a general exposure, standard security measures and medium protection level for the values. Risk levels, shown in the Table 2.2, are first estimations and must be refined for each particular installation. A lot of parameters cannot be determined in advance. E.g., income level of maintenance stuff will heavily influence the rate of attacks from insiders.

| Threat/risk | Metering | SCADA |
|---|---|---|
| direct manipulations of input and output values | high | high |
| manipulation or replacement of equipment | medium | medium |
| manipulation and insertion of data on the Private Network | medium/high | medium/high |
| manipulation and insertion of data on the PLC network | low/medium | low/medium |
| manipulation of Application Server | - | - |
| denial of service | high | high |

Table 2.2 Threats and Risks

Manipulation within an Application Server is out of scope of REMPLI and will therefore not be considered. The Application Servers are trusted entities and intended to be the last instance to report security problems.

Apart from manipulation of data packets, denial-of-service attacks imply a high risk to the system availability, because such attacks can be easily done. For instance, (broadband) disturbers, connected to the powerline network, will easily interrupt powerline communication. On the Private Network the risk of denial of service is also high, and such attacks are well known on the Internet.

The above ratings are valid under the condition that an attacker intends to earn personal profit. If the intention of attacker is vandalism, risk levels must be increased.

 

# 3 Security Concept

This chapter describes the design of the REMPLI security system. Functional safety – also a basic need for a secure system according to the common criteria standard – will not be covered directly, since it is not an issue of a communication system. Nonetheless, the presented measures will also help to improve functional safety. This section describes the security architecture based on classification of data from the previous section. Organisation and responsibilities for security will be discussed in section 4.

There are two principle ways of integrating security into a communication system:

1. Secure tunnel between the end points of communication (e.g., encryption/decryption device placed at each end of the "wire", like HTTP over SSL, RFC 2818);
2. Security enhancements directly in the protocol (like secure HTTP, RFC2660).

In the REMPLI project a hybrid method is used. From the application side REMPLI system should be transparent to application protocols. At least the protocol and the contents of its packets may not be modified. Since many common protocols, used for metering, supervisory and control, do not define security measures and concepts, the REMPLI system must provide means to transport these protocol data units (PDU) securely (secure tunnelling). On the other hand, the REMPLI system defines its own means of transporting data via PLC and, therefore, is able to introduce its own security measures.

This section will start with the definition of boundaries for the security concept and then introduce services and security measures, required at the REMPLI Intranet and PLC – two networks with widely differing performance and threats.

## 3.1 Security Boundaries

Most technical systems (and communication systems in particular) interface with their environment. Therefore, from the security point of view, clear borders have to be drawn before defining security measures.

Since data sources and sinks – e.g. SCADA servers, meters and SCADA equipment – are not defined within the REMPLI project, several assumptions about the system boundaries must be made:

- Metering and SCADA equipment, at the customer's premises is trusted. Protection of this equipment must be done by a proper physical enclosure, which is tamper resistant. If measures to detect tampering (tamper evidence) are included, overall security would be improved.
- All network connections are assumed to be not secure and are therefore not trusted.
- Application Servers (located at the utility company) are trusted. The security measures to protect the Application Servers are out of the scope of REMPLI. If an Application Server offers secure protocols to connect to the interfacing REMPLI device, these protocols should be preferred.
- Finally it is assumed that functionality of the system components (Nodes, Access Point and Bridges) is not manipulated. To fulfil this assumption measures to protect the system components have to be taken.

As shown in Fig. 3.1, all components outside REMPLI (namely, Application Servers and metering / SCADA equipment) are not included into the system and security concept. Networks, connecting these entities, are subject to security considerations, although constraints of these standardized networks must be considered and sometimes even forbid introduction of security measures.

 

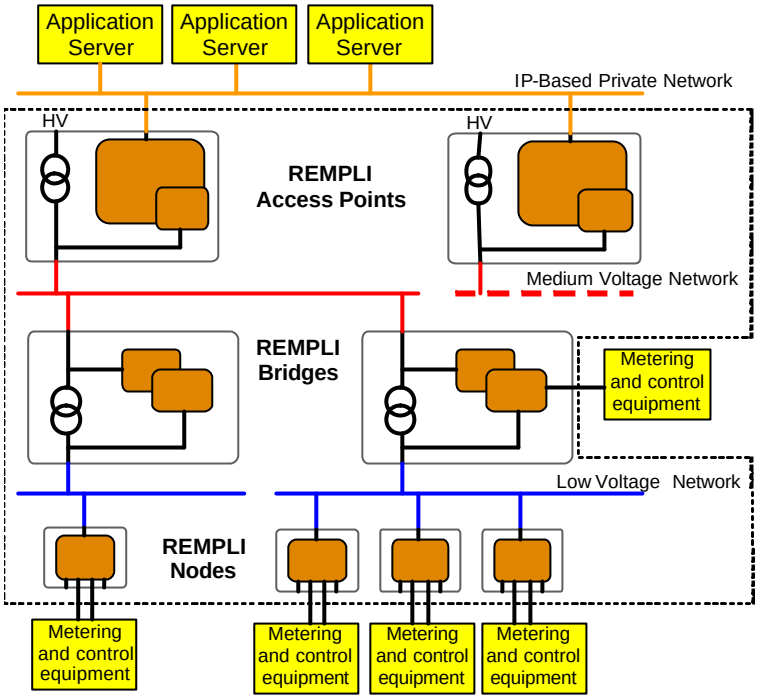


Fig. 3.1 System and security boundaries

According to the analysis of values and risks in section 2 the following services should be offered by the REMPLI system:

1. integrity
2. authentication
3. tamper detection
4. tamper evidence

Cryptographically secure integrity checks must be applied to all information transmitted over the network and to data stored at the nodes, because tamper detection will be based on integrity checks. Additionally, tamper detection will also cover data coming from outside of the system. In particular, data coming from metering or SCADA equipment will be tested for correctness (e.g., new meter reading is less than old meter reading, non-zero meter increments for disabled power terminals, or impossibly high consumption). Mechanisms of tamper evidence include classical measures such as seals and tamper reporting. The latter is a more important instrument since devices of REMPLI are designed for “install and forget” operation. Reporting of system manipulation can either be done within the application protocol, if supported, or by the REMPLI security layer.

Mechanisms for encryption will be included, but there must be a possibility to disable this feature. Non-repudiation is not a primary goal of REMPLI and will only be implemented if there is no performance decrease in the system due to the used mechanism.

## 3.2 REMPLI Communication Security Layer

REMPLI Communication Security Layer is a module within Access Points and Nodes that offers encryption, integrity and authentication services for transmitting packet oriented data over the REMPLI network.

Since a lot of SCADA and metering systems, on the one hand, do not integrate security measures in their protocols and, on the other hand, do not allow changes in the transmitted data packets (e.g. due to certification issues) REMPLI security layer needs to be transparent from the drivers’ point of view. I.e., REMPLI Communication Security Layer treats all traversing data packets as black boxes. Nevertheless, special attention should be paid to the efficient usage in combination with connectionless (packet-oriented) communication, used within REMPLI network to transfer application-layer protocols such as IEC 870-101,

 

IEC 1107, or M-Bus. However, security measures must not rely on specific application-layer protocol, since support for new protocols can be added in the future.

As shown in Fig. 3.2, data transmission in the REMPLI system relies on the concept of paired drivers. Therefore REMPLI Communication Security Layer is also organized in a paired structure below the driver level. The REMPLI Communication Security Layer is integrated at the lower sub-layers of the De/Multiplexer layer of the REMPLI communication system.

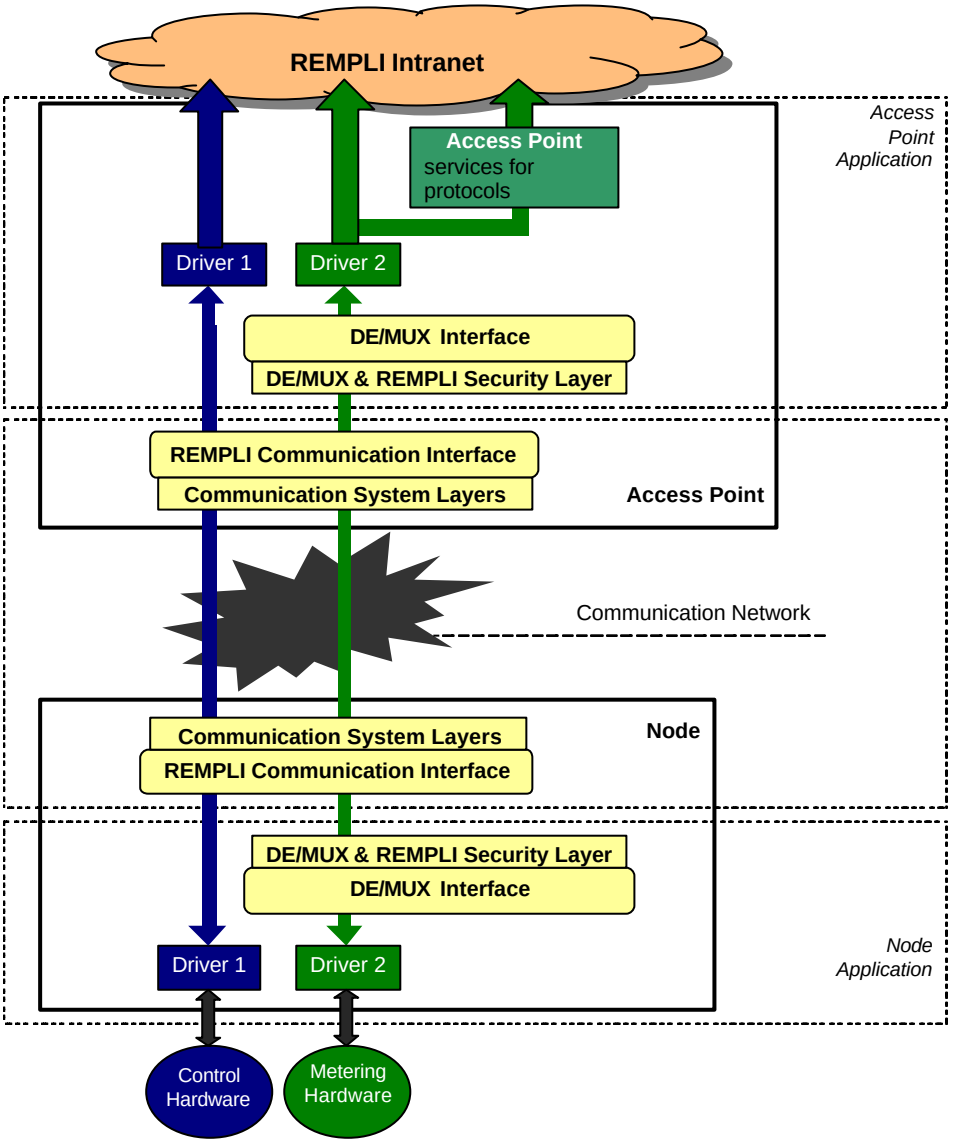


Fig. 3.2 REMPLI Communication Security Layer

The REMPLI system will use PLC as a transport medium. By definition this medium is insecure and the REMPLI PLC system does not offer security measures by itself. Hence, the primary target of the REMPLI Communication Security Layer is to implement all security measures mentioned above with special respect to applications in an embedded environment with real-time capabilities. Additionally, other aspects like limited resources such as bandwidth and computational power should be considered, as long as security is not breached.

In order to fulfil requirements of many different applications, the REMPLI security layer should be configurable in such a way that different levels of security can be implemented. These security levels are:

1. No security ;
2. low security;

3. medium security;
4. high security.

These levels differ in the services they offer (encryption, authentication, integrity,…) and the strength of the used measure. Generally, the higher the security level, the more computational power and resources are consumed. Low-level security will offer integrity and authentication services. For medium-level security also encryption and tamper protection services are added. High-level security includes medium-level measures at the greater strength.

The system must be capable of running services of different security levels in parallel, although some systems might only use one kind of service. The level of security is chosen on a driver level, e.g. a IEC 1107 driver might use high security level whereas an IEC 60870-5 driver uses low security. The concept of parallel security levels can even allow for a PDU oriented selection of security measures and strength.

### 3.2.1 Performance Considerations

Calculations on the overhead of security measures clearly shows that the amount of overhead extremly depends on the actual payload. Assuming a constant encryption block size of 16 bytes (common DES – Data Encryption Standard – and 3-DES) and a MAC of 16 bytes, the overhead for large packets like weekly or monthly load profiles (20 to 50kByte) is very low. For small packets with only a few bytes or bits the situation is different and security measures introduce a big amount of overhead. Nevertheless, these services are the most important ones to guarantee security and liability of the system. If these fields are reduced security will be flawed.

### 3.2.2 Configuration

Configuration starts with a personalisation phase at manufacturing time[1] of the REMPLI device. This is the only time when configuration data has to be uploaded locally to allow for initial communication. From security point, this phase is the most dangerous, because root-security information must be transmitted unprotected. All further security measures will rely on the integrity and confidentiality of these root secrets (e.g. general maintenance key). Subsequent configurations will be done remotely via management interface of the Access Point. Changes will be propagated to the Node side of REMPLI Communication Security Layer via security management messages. For these operations the highest security level must be always applied.

### 3.2.3 REMLI Private Network Security Layer

Differently from the PLC network, where security protocols have to be optimized to fulfil the performance requirements, security measures for protecting transmissions on the Private Network offer more choice, since it is an IP-based network with a higher bandwidth than the PLC. Hence, usage of standard Internet security algorithms and services will be favoured. The advantages of standard Internet security measures are the easier integration at the utilities' Application Servers and that these measures are already well tested in the Internet. Integration at the Application Server is a very important topic due to the fact, that Application Servers are expensive software, bound to a certain operating system. Changes at the Application Servers are considered to be very complicated in respect to installation and maintenance.

### 3.2.4 Local Maintenance and Maintenance Terminal

In general, maintainace is performed remotely, as REMPLI devices are designed for "install and forget" operation. Nonetheless, possibility for local maintenance must still remain. The security of (local) maintenance will use the same authentication, encryption and integrity measures as for remote administration.

[1] According to the concept of REMPLI devices, there should be no configuration during in-site installation. In-site configuration demands to provide a lot of system information to skilled personal. This overhead should be avoided.

For low-security normal maintenance keys can be calculated from username and password. In case of medium to high security maintenance tasks, authentication and access control stronger than the previous scheme must be used (e. g. smart card).

## 3.3 Security measures

This section describes the security functions to be used to achieve security goals of the REMPLI system.

### 3.3.1 Cryptographic Algorithms

The REMPLI system offers three basic security services: confidentiality, integrity, and authentication. To achieve these goals cryptographic algorithms will be used.

The challenge in the REMPLI (security) system is to cope with the limited bandwidth, the packet-oriented data transmission in the PLC, and the limited resources on the nodes. Typical PLC packet sizes are 32 and 64 bytes and typical application data size is between 10 bytes for single commands and meter readings and 50 kbytes for profiles. Therefore, making use of standard Internet security measures often implies problems in bandwidth efficiency and computational power. Depending on the security level different crypto algorithms will be facilitated in respect to their usage. Symmetric as well as asymmetric block ciphers and hash functions will be used. Stream ciphers turned out to be less feasible since they imply a high synchronisation effort on the PLC, which by nature is prone to packet loss.

Looking at the actual research results, symmetric ciphers are favoured for normal workload due to their better efficiency. On the management level (including regular exchange of working keys) there is little difference between asymmetric and symmetric algorithms.

### 3.3.2 Access Control and Authentication Services

Since the REMPLI system can be used by multiple users, access control measures must be applied. Access control handles rights of a user to access an object of a metering or SCADA device. Therefore the user and the target object must be identified. Since metering and SCADA protocols are in general not built to share[2] a communication system, the only information in general available at the Access Point is the IP-address of the Application Server. Hence, identification of the user is done by identifying the Application Server that sends a request or receives an alarm. For those applications, which allow authentication by other means (e.g. username/password), these measures should be used additionally. Access control of data points (objects) will be handled on a driver basis, because only the driver knows all characteristics of the protocol like object adresses.

Access control is handled by lists of Access Point-object pairs. Since contents of the lists is protocol specific and depends on resources, possible solutions vary from protocol to protocol and can range from look-up tables to databases. For universal and resource efficient usage the lists should support

1. ‘forbiddance’ entries, which will be used to prohibit access for a specific subset of objects;
2. ‘allowance’ entries, which only grant access to a small subset of objects.

Access control relies on the correct verification of the origin of a message. It is therefore important that the entity which sent the packet (Application Server, Node, Access Point) authenticates itself properly. If this Authentication is missing the access control can be easily circumvented.

Concerning the resources (in particular memory) these measures consume, a trade off between granularity and costs must be found. Since the REMPLI field test is not fully defined yet, only estimations can be given here. Concerning authentication, a maximum of 12 service providers (maximum of three competing providers for the utilities water, heat, electricity and gas) and a maximum of 50 objects[3] is assumed.

[2] Share in a way that everyone has access to every object.

[3] According to the extend of the REMPLI fieldtest.

### 3.3.3 Physical Protection of Devices and Security Token

Equipment should be tamper resistant and tamper evident. Therefore the case of every device must be designed in such a way that

- manipulation of the enclosed equipment is not possible from the outside and
- manipulations and opening of the case are detectable

Since REMPLI is not a high-security application, the trade off between costs and security will, for economical reasons, favour cost optimisation rather than security. Hence, only simple measures are applicable within boundaries of the security policy. More advanced features that cannot be circumvented easily, like active tamper protection shields, are too cost intensive for the application. Physical protection will include seals – mainly needed for legal purposes – mechanical protection of the case and integration of a security token.

Different to the microprocessor of the node, where data can be easily analysed, the security token is designed in such a way that an attacker cannot reveal the secrets stored on the security token even if he/she has a permanent phyiscal access to the security token. Within REMPLI each node contains a smart card as a security token for key storage and crypto processing.

### 3.3.4 Key System Architecture

REMPLI uses a multi-layer security (key) system, in which several different keys are implemented. If a key at one level is compromised, this system allows to remotely replace the broken key from a higher security level. Therefore each layer is independent of the previous layer.

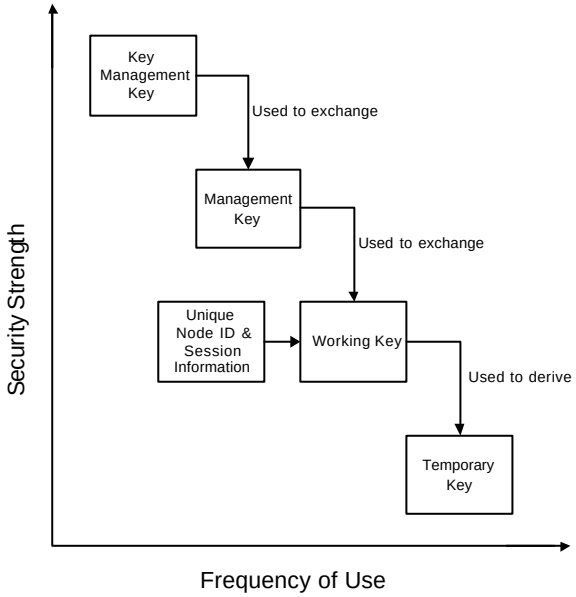


Fig. 3.3 Key system overview

The system implements four layers of security (see Fig. 3.3):

1. Key management level: Highest level security, used to exchange new management keys. Key storage and cryptographic calculations using these keys are only done inside the security token. These keys are directly installed during personalistion of the security token.
2. Management level: The task of the management level is to securely exchange working keys that are used to exchange new working keys for transmission of payload data. Operations at the management level will also be done inside the security token, but there is a possibility to remotely configure and update the keys of the management level.

 

3. Working level: The keys of the working level can either be used to encrypt and authenticate payload data or to derive new temporary keys.
4. Temporary Key level: These keys are used for every day communication. As a commitment to the performance and resource gap between a security token and a host processor these keys might be stored and used outside the security token. To keep the risk of misuse low, Temporary Keys are only valid for a maximum of one day.

## 3.4 Additional Security Tasks

Additional security tasks depend on the actual application and therefore are outside of REMPLI security layers. These tasks primarily include mechanisms for tamper protection of inputs to the REMPLI system, such as

- raising alarms if out-of-bounds parameters are detected (e.g. wrong metering values);
- determining, if metering and SCADA equipment is still reachable and operational; and
- determining, if semantically incorrect values are supplied by the equipment.

Tasks implemented heavily depend on the metering and SCADA equipment used.

 

# 4 Integration into the Company Security Policy

A security policy includes technical and organisational security relevant issues of the system. Within the REMPLI project, and therefore also within this document, only the technical aspects for a standard metering and SCADA scenario with a low to medium threat level are described. A complete security policy can only be defined for a particular application and within the security policy of all pariticipants using the system.

Special issues to be handled in the organisational part that are relevant for the technical implementation are:

1. Responsibilities: Clear responsibilities must be set up for the tasks that are not automatically done by the system, but also for tasks that affect the system, like maintenance and installation. A role model with restrictive responsibilities is favourable since the threat from insiders (service providers and system operators) has the same level as from external persons (customers and third parties).
2. Security centre: The security centre is a synonym for the organisational unit that is responsible for generation and distribution of credentials (keys) and authentication of data that affects system configuration. Furthermore, it shall act as an entity to which security relevant information, such as manipulation alarms, can be delivered. The security centre can redistribute this task to other entities if applicable.
3. Security management: This topic will include all actions after installing the security system. It includes key management, security issues of software updates (change management) but also tasks like continuous security analysis and adaptation of measures, if vulnerabilities have been discovered.
4. Acceptance of security measures and residual risk: The residual risk is defined by the residual risk of the used algorithms, the security schemes applied, and the acceptance of the security measure by the end-user. Following the first rule of security (principle of Kerkhoff) the system only uses well-known and analysed algorithms. This decision strongly reduces the residual risk of algorithms and security schemes, because cryptographic community assumes such standard algorithms and procedures to be secure. This assumption is based on the fact that up to now no known vulnerabilities exist and that for the next years it will be (computationally) infeasible to tamper the system by brute-force attacks. User acceptance has a bigger influence on security especially if non-security personal is involved (e.g., local maintenance personal). Security measures must be designed in an appropriate way.

 

# Glossary

| | |
|---|---|
| AES | Advanced Encryption Standard |
| APDU | Application Protocol Data Unit |
| ASCII | American Standard Code for Information Interchange |
| CBC | Cipher Block Chaining |
| CC | Common Criteria |
| CIA | Confidentiality, Integrity, Authentication |
| DES | Data Encryption Standard |
| DSA | Digital Signature Standard |
| ECB | Electronic Code Book |
| ECC | Elliptic Curve Cryptography |
| ECC | Elliptic Curve Cryptosystems |
| GPS | Global Positioning System |
| GSM | Global System for Mobile Communication |
| HV | High Voltage |
| I/O | Input/Output |
| IDEA | International Data Encryption Standard |
| IEC | International Electrical Commission |
| IEEE | International Electrical and Electronic Engineers |
| IP | Internet Protocol |
| IPSEC | IP Security Protocol |
| ISDN | Integrated Service Data Network |
| IT | Information Technology |
| LUT | Look-Up Table |
| LV | Low Voltage |
| MAC | Medium Access Code |
| M-BUS | Metering Bus |
| MV | Medium Voltage |
| NIST | National Institute of Standards and Technology (USA) |
| OFB | Output Feedback |
| PDU | Protocol Data Unit |
| PL | Power line |
| PLC | powerline communication system |
| PLL | Phased Locked Loop |
| POTS | Plain Ordinary Telephone System |
| PPM | parts per million |
| PTB | Physikalisch-Technische Bundesanstalt |
| RAM | Random Access Memory |
| RCI | REMPLI Communication Interface |
| RKEP | Remotely Keyed Encryption Protocol |
| ROM | Read Only Memory |
| RSA | Rivest Shamir Adleman cryptographic algorithm |
| SAR | Segmentation and Reassembly |
| SCADA | Supervisory Control And Data Acquisition |
| SHA | Secure Hash Algorithm |
| SSL | Secure Socket Layer |
| SSN | Security Sequence Number |
| TCP | Transport Communication Protocol |

 