# Chapter 4

# SYSTEM SPECIFICATIONS

## 4.1 SECURITY POLICY OVERVIEW

Many systems that need security are concerned one way or another with monitoring some aspect of the environment. They range from ordinary domestic burglar alarms through utility meters to tachographs, and even a number of systems critically concerned with nuclear safety. The protection of these systems is most often more concerned with preventing attacks that involve denial of service, such as swamping communications, overwhelming sensors. Service denial attack might be complemented with various kinds of data manipulations. Systems may have to deal with numerous mutually suspicious parties, and often are implemented using the cheapest possible microcontrollers. Many of these systems are continually in the hands of the enemy. Key management is an important consideration, especially in low-cost widely distributed systems where a central key management facility cannot be justified. The services required are determined from the functional requirements to be met and risks that must be addressed. The possible security services are:

- S1: Access Control
- S2: Authentication
- S3: Confidentiality
- S4: Integrity
- S5: Non-repudiation
- S6: Availability

Table 4.2 shows the various functional requirements and the security service that will be needed to make ensure that each requirement is met.

## 4.2 SYSTEM COMPONENTS

In order for a security policy to be successfully implemented each component of the system must address certain security aspects. In section 3.2.1 the system's main components were identified. Threats to each of these components, with regards the functional requirements, were listed in section 3.2.3. This section explains where security services must be implemented in order to mitigate threats to the system assets and functional requirements.

**Table 4.2:**
**Functional Requirement vs Service mapping**

| | S1 | S2 | S3 | S4 | S5 | S6 |
|---|---|---|---|---|---|---|
| F1 | | | | | | X |
| F2 | | | | | | X |
| F3 | | | | | | X |
| F4 | | | X | | | |
| F5 | | X | | | | |
| F6 | | X | | | | |
| F7 | | X | | | | |
| F8 | X | X | | | | |
| F9 | X | X | | | | |
| F10 | | | | X | | |
| F11 | | | X | | | |
| F12 | | | | | X | |

### 4.2.1 Node

In order to facilitate security services the node needs to have the ability to perform cryptographic operations, e.g. encrypt/decrypt, hash and generate random numbers. The node also needs to store some information pertaining to the respective security services: data about some nodes, the gateway, its owner and its user. To prevent replay attacks the node must keep track of communication sequence numbers and time-stamps (needs a clock). Mapping of applicable threats to security services are shown in table 4.2.1.

- N1: Denial of service attacks at the node will mostly be of a physical nature. Nodes must be physically secure to prevent access to security and functional hardware.
- N2: If the node accepts and processes malicious information it will be prevented from providing a valid service. If it is controlling a critical operation the consequences will be disastrous. Nodes must be able to verify the integrity of all information received.
- N3: Information release does not effect the operation of the node but does effect its owner. A malicious entity could intercept sensitive information about business oper-

ations and sell it to competitors. The node must secure all information transmitted or received.

- N4: If a malicious owner convinces a node that it is legal then that owner can disrupt the system or gain sensitive information. Authentication procedures must be secure and ensure that only legal entities are authenticated.
- N5: If a malicious user convinces a node that it is legal then that user can gain access to services. Authentication procedures must be secure and establish the identity of the user correctly.
- N6: A legal owner might try to access information that it is not allowed to see. Information must be labelled and access control implemented at the node in order to determine what the owner may access.
- N7: A legal user might try to access information that it is not allowed to see. Information must be labelled and access control implemented at the node in order to determine what the user may access.
- N8: If the user or the owner denies that a transaction or service took place there must be sufficient proof to settle the dispute. The owner and the user must be successfully identified and some secret information from both must be used to bind both entities to a transaction.

**Table 4.2.1:**
**Threats: Node vs Service mapping**

| | S1 | S2 | S3 | S4 | S5 | S6 |
|---|---|---|---|---|---|---|
| N1 | | | | | | X |
| N2 | | X | | X | | |
| N3 | | | X | | | |
| N4 | | X | | | | |
| N5 | | X | | | | |
| N6 | X | X | | | | |
| N7 | X | X | | | | |
| N8 | | | | | X | |

### 4.2.2 Private Network

In order to facilitate security services the network needs to provide some information: destination ID, source ID, acknowledge flag, end of message flag, multicast flag and sequence number. Most fieldbus protocols only define the operation of the lower 2 layers of the OSI model. Therefore a network and transport layer must be implemented to provide an addressing scheme and connection-oriented communication. Mapping of applicable threats to security services are shown in table 4.2.2.

- FAN1: If a malicious node gains access to the network and convinces other entities that it is legal then that node can disrupt the system or gain sensitive information. Procedures must be implemented to ensure that only valid nodes reside on the network.
- FAN2: If a malicious node successfully appears to be another legal node then that node can gain access to services. Authentication procedures must be secure and establish the identity of the node correctly.
- FAN3: If a node or gateway accepts and processes malicious information it will be prevented from providing a valid service. All entities must be able to verify the integrity of all information received.
- FAN4: Information release does not effect the operation of the network but does have consequences. A malicious entity could intercept sensitive information about network operations and use it in future attacks. All information transmitted or received must be secured by network entities.
- FAN5: If a malicious node gains access to the network and convinces other entities that it is legal then that node can disrupt the system or gain sensitive information. Authentication procedures must be secure and ensure that only legal nodes can reside on the network.

**Table 4.2.2:**
**Threats: Private Network vs Service mapping**

| | S1 | S2 | S3 | S4 | S5 | S6 |
|---|---|---|---|---|---|---|
| FAN1 | X | X | | | | |
| FAN2 | | X | | X | | |
| FAN3 | | | | X | | |
| FAN4 | | | X | | | |
| FAN5 | | X | | | | |

### 4.2.3 Public Network

The protocols in the public network are well known and provide services for the 3rd and 4th layer of the OSI model already. Therefore existing functionality can be used. Mapping of applicable threats to security services are shown in table 4.2.3.

- PN1: Denial of service attacks on the network infrastructure cannot be addressed by the security policy. The only solution is to choose a reliable third party network operator with a sound security policy pertaining to availability.
- PN2: If a gateway or owner accepts and processes malicious information it will be prevented from providing a valid service. All entities must be able to verify the integrity of all information received
- PN3: Information release does not effect the operation of the network but does have consequences. A malicious entity could intercept sensitive information about network operations and use it in future attacks. All information transmitted or received must be secured by the communicating entities.
- PN4: Although no sensitive data is released an attacker can still gain information about network topology or the nature or frequency of transactions from control information, e.g. addresses, time-stamps, etc. The communication must be secured in a way such that some control information is hidden but the public network can still process the packets.

**Table 4.2.3:**
**Threats: Public Network vs Service mapping**

| | S1 | S2 | S3 | S4 | S5 | S6 |
|---|---|---|---|---|---|---|
| PN1 | | | | | | X |
| PN2 | | | | X | | |
| PN3 | | | X | | | |
| PN4 | | | X | | | |

### 4.2.4 Gateway

In order to facilitate security services the node need to have the ability to perform cryptographic operations, e.g. encrypt/decrypt, hash and generate random numbers. The nodes also needs to store some information pertaining to the respective security services: data about the nodes on its network and their owner. To prevent replay attacks the node must keep track of communication sequence numbers and time-stamps (needs a clock). Mapping of applicable threats to security services are shown in table 4.2.4.

- G1: Denial of service attacks at the gateway can be physical or originate from either the private or public network. The gateway should be physically secure if possible. Resource sharing must be managed in such a way that it impossible for one entity to tie up the gateway. The gateway should only accept service requests from authenticated entities that are less likely to disrupt services.

- G2: A legal node might try to request information from an owner that it is not allowed to see. Information must be labelled and access control implemented at the gateway in order to determine what services the node may request.

- G3: A legal owner might try to access nodes which it is not allowed to. Nodes must be labelled and access control implemented at the gateway in order to determine what the owner may access.

- G4: If a malicious node convinces the gateway that its legal then that node can gain access to services. Authentication procedures must be secure and ensure that only legal nodes can reside on the network.

- G5: If a malicious owner convinces the gateway that it is legal then that owner can gain access to the private network. Authentication procedures must be secure and ensure that only a legal owner can access the private network.
- G6: The gateway has access to all owner-node communication. A physical or software attack might try to gain access to the gateway in order to monitor, modify or disrupt communications. The gateway must be physically secure and a trusted administrator must ensure its operation. Unauthorized software installations or data access must not be allowed.

**Table 4.2.4:**
**Threats: Gateway vs Service mapping**

| | S1 | S2 | S3 | S4 | S5 | S6 |
|---|---|---|---|---|---|---|
| G1 | | | | | | X |
| G2 | X | X | | | | |
| G3 | X | X | | | | |
| G4 | | X | | | | |
| G5 | | X | | | | |
| G6 | X | | X | X | | |

### 4.2.5 Owner

In order to facilitate security services the owner needs to have the ability to perform cryptographic operations, e.g. encrypt/decrypt, hash and generate random numbers. The owner also needs to store some information pertaining to the respective security services: data about its nodes and the gateway. To prevent replay attacks the owner must keep track of communication sequence numbers and time-stamps (needs a clock). Mapping of applicable threats to security services are shown in table 4.2.5.

- O1: Denial of service attacks at the gateway can be physical or originate from the public network. The owner IT infrastructure is governed by its security policy. The owner is responsible for ensuring availability.
- O2: If a malicious entity convinces an owner that it is legal then that enity can disrupt the system or gain sensitive information from the owner. Authentication procedures must be secure and ensure that only legal entities are authenticated.

- O3: A legal node might try to request services that it is not allowed to. Services must be labelled and access control implemented by the owner in order to determine what the node may access.
- O4: A legal gateway might try to request information on behalf of a network which is not entitled to that information. Access control must be implemented by the owner in order to determine if the gateway may request a service, e.g. labeling the data with security levels and preventing entities to access data with higher clearance.
- O5: Attackers will attempt to access sensitive information communicated between the owner and its nodes. Information transmitted or received must be secured.
- O6: If the owner accepts and processes malicious information it will be prevented from providing a valid service. The owner must be able to verify the integrity of all information received.
- O7: If the node or the owner denies that a transaction or service took place there must be sufficient proof to settle the dispute. The owner and the user must be successfully identified and some secret information from both must be used to bind both entities to a transaction.

**Table 4.2.5:**
**Threats: Owner vs Service mapping**

| | S1 | S2 | S3 | S4 | S5 | S6 |
|---|---|---|---|---|---|---|
| O1 | | | | | | X |
| O2 | | X | | | | |
| O3 | X | X | | | | |
| O4 | X | X | | | | |
| O5 | | | X | | | |
| O6 | | | | X | | |
| O7 | | | | | X | |