Chapter 3

SYSTEM OVERVIEW

3.1 SYSTEM DEFINITION

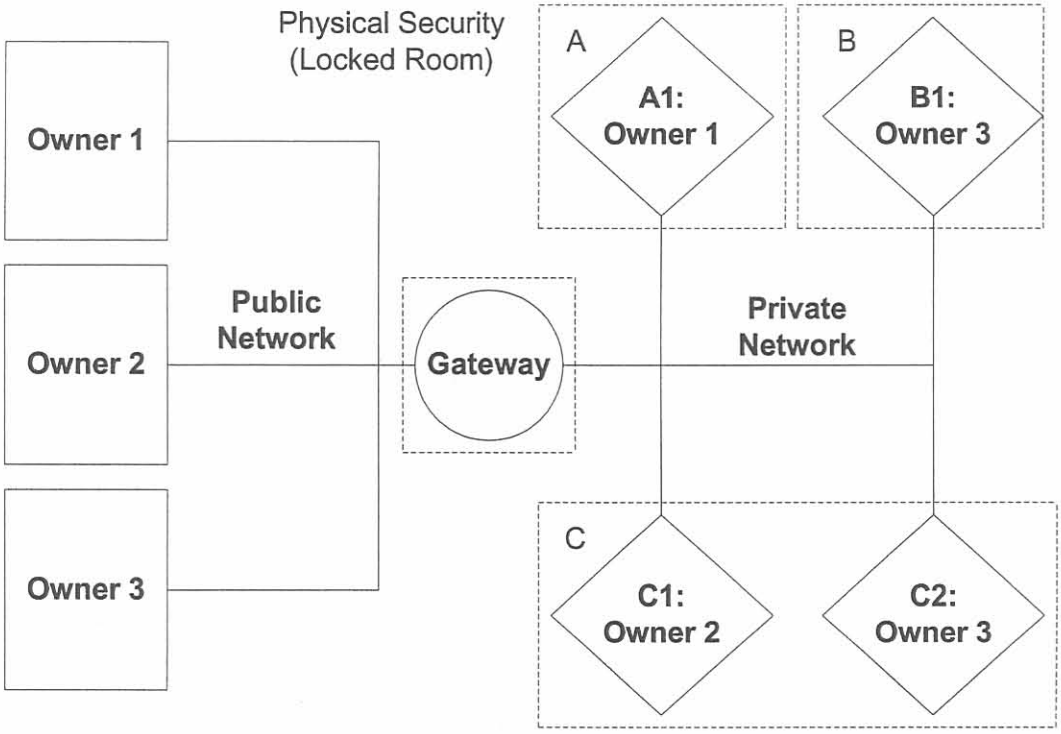

Figure 3.1:
System Model

The general configuration for a possible field area network, connected to a public network, is shown in figure 3.1. The public network allows for different entities to access the private network from remote locations. The private, or field area network, is responsible for connecting the entities located at the users' premises. This dissertation will refer to entities on the private network as nodes, to the entities in the public network as owners (owners can utilise the node to gain information or to provide a service) and to the entity linking the two networks together as the gateway. Such a system is extremely versatile, it accommodates various setups and both the user and the owner can make requests for a service or data. This can be applied in multimedia systems, prepaid systems and commercial applications (e.g. the user could request a service online which then causes its node to be enabled) [8]. The private network is not autonomous. Entities from different owners or

entities with different users may be connected to the same private network. Each entity needs a secure way to relate to its owner, user and peers in the network without being compromised [2].

3.1.1 System Architecture

The following system entities can be identified (please refer to figure 3.1):

- Premises A, B and C. These are areas controlled by different users, e.g. a single room, an area of a factory and a single house or flat.
- Embedded nodes A1, B1, C1 and C2. Located at premise A, B and C respectively, these nodes provide service to the local user.
- The private network (FAN) provides a communication medium between the nodes and the gateway.
- The gateway connects the private network to the public network. It is unlikely that the private and public networks utilize the same protocols and therefore the gateway can also be seen as protocol translator.
- Owners 1, 2 and 3. These entities access the nodes they own in order to provide services to the users.
- The public network allowing remote access to the gateway by the service providers.
- The user who benefits from the action of a node.

3.1.2 Assumptions

In order to focus on the problem area the boundaries of the system need to be defined. In order to limit the system certain assumptions need to be clarified:

- Premises:
  1. The premises are physically secure.
  2. The nodes cannot be physically accessed by anyone except the user.
  3. A premise might contain nodes related to different service providers.

- Nodes:
  1. Nodes on the same private network can communicate with one another.
  2. Nodes communicate with the gateway to facilitate communication with its owner.
  3. A node only communicates with its owner to receive instructions and relay information.
  4. The node's owner and user might not be the same entity.
  5. A node only has one owner.
  6. A node only has one user.
  7. A node is physically secure.
  8. A node has low processing and storage resources.
  9. A node's software cannot be altered after implementation.
  10. The node is limited in what security services it can provide.
  11. A node is not a trusted entity.
  12. The frequency of communications between nodes can be high and consists of short data streams.
- Field Area Network:
  1. The implemented private network infrastructure spans multiple premises.
  2. A central IT management structure controls possible addressing schemes and the gateway.
  3. Low-bandwidth, connectionless message based communication, e.g. CANBus, Profibus, LonWorks.
  4. Communication standard only specifies layer 1 and 2 of the OSI model.
  5. Broadcast or bus architecture, which means all entities on the network receive all data transmitted.
- Gateway:
  1. There is only one gateway in the system for each field area network.
  2. The gateway is a trusted entity if adequate physical security is ensured.

3. The gateway is untrusted when adequate physical security cannot be ensured.
4. The gateway has sufficient resources to implement any security service.
5. The gateway only relays data or executes commands from a service provider.
6. The gateway needs only to communicate with owners that own nodes on the private network.

- Owner:

1. Communicates with the nodes on different private networks.
2. Communicates with different gateways.
3. The owner is a trusted entity.
4. The frequency of communications between an owner and a node is low and consists of long data streams.

- Public Network:

1. Public infrastructure, e.g. Internet.
2. High bandwith communication, connection oriented communication, e.g. probably TCP/IP.
3. The operation of this infrastructure is ensured by a third party and is not the responsibility of either the user or the owner.

3.2 RISK ANALYSIS

In order to perform a risk analysis the assets and the basic functional requirement of the system must first be identified. Adequate safeguards must be implemented to protect the assets and ensure that the functional requirements are met. Vulnerabilities and threats need to be identified in order to determine which safeguards our policy must implement [50].

3.2.1 Identification of Assets

Information is the most important as the whole system is implemented in order to share information between entities for the purpose of making correct decisions in providing functionality. If data was to be corrupted or prevented from reaching its intended recipient the network would not be able to function correctly. Therefore all assets are rated

according to their ability to maintain successful data flow. The system assets, in order of importance, are as follows:

1. Nodes: Allow users to access the network and obtain several services. If the users cannot gain access to the network the system is no longer functional as it has no purpose. Nodes also store and manipulate data to provide useful information. If a node is prevented from functioning correctly all functionality is lost.

2. Private network infrastructure: Allows the nodes to communicate with another in order to provide functionality within a limited geographic area. Disruption of the private network is disastrous as nodes cannot obtain information or supply information that might be critical to the overall function of the network, e.g. a central air conditioner might require temperature readings from various sources in order to make adjustments. Functions that rely on a single node will still have limited functionality, e.g. a valve regulating a cooling tank might keep the water level correct but will not be able to accept changes or report water level readings to it owner.

3. The gateway: Although not providing any services the gateway is solely responsible for all traffic flow between the networks. Failure in the gateway will therefore seriously limit connectivity and data flow outside the private network. The gateway is also centrally located which makes it a viable centre of operations for security services.

4. Public network infrastructure: This network allows the owner to access its nodes and provide a service. Due to the nature of distributed embedded systems (the functionality is provided locally as far as possible) the private area network and its applications will still function. However, the owner won't be able to access the node in order to retrieve information or make changes to its services.

5. The owners: Although actions by the owners are not as critical as the actions made by the nodes these entities still provide and require services from their nodes that are necessary for overall system functionality.

3.2.2 System Requirements

The following functional requirements necessary for system operation can be identified:

- F1: Two nodes must be able to communicate with one another.

- F2: A node must be able to communicate with the gateway.
- F3: An owner must be able to access its node when required.
- F4: The gateway, a unauthorized node or a unauthorized entity on the public network must not be able to gain useful information from a communication sequence between a node and another authorized node, or a node and its owner.
- F5: A node needs to be authenticated by other nodes and its owner.
- F6: An owner needs to be authenticated by its nodes and the gateway.
- F7 A untrusted gateway must be authenticated by the owner.
- F8: The gateway must relay valid messages between the private and public network without being able to disclose information within those messages.
- F9: An owner, node or gateway may gain access to any system resources illegally.
- F10: Entities must be assured of the integrity of any information transmitted.
- F11: Information and services are private and may not be disclosed.
- F12: Necessary proof must be provided in order to settle disputes between parties.

3.2.3 Vulnerabilities and Threats

Vulnerabilities are aspects of the system which can be exploited. Threats can be seen as possible ways in which these vulnerabilities can be exploited to undermine the functional requirements [51]. The areas of vulnerability, with associated threats, can be listed as follows:

1. Node
   - N1: Denial of service attack.
   - N2: Use of modified data or data from a malicious source.
   - N3: Release of message contents between node and another authorized entity.
   - N4: Authentication of a malicious owner (masquerade, replay attacks).
   - N5: Authentication of malicious user.

- N6: Unauthorized owner being allowed to access services to which he/she is not entitled.
- N7: Unauthorized user being allowed to access services to which he/she is not entitled.
- N8: User or owner of node denying that service was received or requested.

2. Private Network (FAN)

- FAN1: Node or malicious entity gaining access to a network which it is not entitled to.
- FAN2: Illegal node pretending to be another legal node.
- FAN3: Modification of data sent or received.
- FAN4: Release of message contents between entities on the network.
- FAN5: Authentication of a malicious node on the Private Network (masquerade, replay attacks).

3. Public Network

- PN1: Denial of service attack on the public network infrastructure cannot be addressed.
- PN2: Modification of data sent or received.
- PN3: Release of message contents between owner and private network.
- PN4: Traffic analysis on public network.

4. Gateway

- G1: Denial of service attack (private/public network side).
- G2: Node gaining illegal access to public network and owners.
- G3: Outside entity (or owner) gaining illegal access to private network and nodes.
- G4: Authentication of a malicious user or node on the private network (masquerade, replay attacks).
- G5: Authentication of a malicious owner on the public network (masquerade, replay attacks).

- G6: Attack of the gateway in order to gain access to owner-to-node communication.

5. Owner

- O1: Denial of service attack
- O2: Authentication of a malicious node/gateway (masquerade, replay attacks).
- O3: Illegal node gaining access to service to which it is not entitled.
- O4: Illegal gateway gaining access to services to which its network is not entitled.
- O5: Release of message contents between owner and gateway/node.
- O6: Modification of data between owner and gateway/node.
- O7: User node denying that service was received or requested.

Only vulnerabilities of technical nature will be considered, therefore threats as a result of personnel security, business management or training inefficiency are ignored. Table 3.2.3 shows the final risk analysis of the system. Likelihood of occurrence is mapped versus severity if the threat should realise. Overall importance is numbered from 1 to 9, with 1 being the most important.

Table 3.2.3:
Risk analysis for distributed system

	Frequent	Not often	Seldom
High	**1** N1, G1	**2** N2, FAN6, PN1, G3, O1	**3** N4, N5, N8, G6
Medium	**4** FAN1, FAN2, PN2	**5** N7, FAN5, PN3, G4, G5, O5	**6** N6, O4, O7
Low	**7** FAN3, FAN4, O2, O3	**8** N3, G2, O6	**9** PN4