Proceedings of the 17th World Congress
The International Federation of Automatic Control
Seoul, Korea, July 6-11, 2008

Secure Virtual Automation Networks based on a Generic Procedure Model

M. Wolframm*. H. Adamczyk**

** Teleport Sachsen-Anhalt, Barleben, 39179*
Germany (Tel: +49-39203-82549; e-mail: mario.wolframm@tsa.de).
*** Institut f. Automation und Kommunikation Magdeburg, Barleben, 39179*
Germany (Tel: +49-39203-81066, e-mail: heiko.adamcyk@ifak.eu).

Abstract: Security is a huge topic, however an international standard for automation control systems is missing. The standardisation work is progressing, e.g. within the IEC. It is clear that behind security there are several well-known security objectives such as availability, integrity and confidentiality. It is also clear that the office domain provides thousands of different security solutions. A possible use for automation networks, 1 to 1 or with adaptations, is one task within the VAN project. Furthermore VAN sets its focus on IT-Security and thereby on communication security. The use of the brand-new procedure model which is part of the VDI/VDE guideline 2182 was applied. The first time use of this model was a challenge and also a benefit for the project.

1. INTRODUCTION

In the beginning of the working package 6 Security in the VAN project, it was difficult to catch the cross-platform topic which stands behind Security. Our first focus was on IT-Security and then to concentrate only on the communication security aspects. This was a basic decision. Nevertheless with this focus in mind it was not easy to develop a systematic approach which also has the claim to cover all IT-Security aspects and to specify and develop a secure VAN system.

One solution was to take the brand-new procedure model of the VDI/VDE Guideline 2182 (VDI/VDE, 2007). Originating from the plan-do-act-check model, the German national committee 5.22 “Security” within VDI/VDE Gesellschaft Mess- und Automatisierungstechnik (GMA) has developed a dedicated model for the use within industrial automation. This model was compiled by 25 experts (manufacturer, machine builder, industry, research institutes) and it is in the form of a guideline. It describes how specific measures (organisational, technical) can be implemented in order to guarantee the IT-Security of a specific automation device or system. This model was applied to a VAN system approach. Some first experiences are given in this paper.

1.1 Basic Security Objectives

Described below are the definitions which are necessary to have a solid understanding of the topic IT-Security. This means VAN considers only information Security in a given IT infrastructure.

Availability:
The probability that a target of inspection will be in a state which will allow it to fulfil a required function under the specified condition at a specified time or during a specified period.

Confidentiality:
Confidentiality is the characteristic which means that data or information contained can only be accessed by authorised users.

Integrity:
Integrity is the characteristic which means that unauthorised users cannot create, modify, replace or delete data unnoticed.

Authenticity:
There are two basic types of authenticity: user authenticity and data authenticity. User authenticity means that a user really is who he or she claims to be. The corresponding check is called authentication. Data authenticity means that data really did originate with the specified sender or creator and has not been modified during transmission. Data integrity is part of data authenticity.

Non-repudiability:
Non-repudiability is the characteristic which means that the target of inspection is able to retrospectively name the originator of an action (demonstrable).

Auditability:
Auditability means that (selected) actions are recorded so that the complete chronological sequence of events can be traced back. It is advisable when recording an action to also specify the corresponding originator.

978-1-1234-7890-2/08/$20.00 © 2008 IFAC

10.3182/20080706-5-KR-1001.1728

1.2 Status of IT-Security in the Industrial Automation

Authentication and Authorisation are the prerequisite for each security solution. Authentication determines whether someone is really the person he claims to be. Authorisation determines what someone is allowed to do. Cryptographic algorithms provide the basis for communication security. They help to provide confidentiality and integrity. Also authentication heavily relies on cryptographic algorithms. Current cryptographic techniques use keys for encryption and decryption. Certificates help to handle keys.

Authentication, Authorisation and cryptographic techniques are the building block for security solutions of communication security like firewalls and IPsec. Furthermore these building blocks are increasingly used within more or less closed wireless systems (e.g. ZigBee as an example of a wireless sensor network). Beyond that, keys are a very important part for all cryptographic algorithms. VAN considers two dominated techniques for key distribution. One of these is the use of a public key infrastructure.

1.3 Network and System IT-Security Aspects

Starting from the device level, an overall IT-Security solution contains a set of several technical as well as organisational measures. That is why IT-Security is a system approach. From the IT infrastructure point of view, a system is represented by a given number of devices connected via a network (e.g. virtual area network).

2. GENERIC IT-SECURITY MODEL

2.1 Overview

The method is like a uniform, feasible procedure for ensuring IT-Security throughout the entire life cycle. The process consists of 8 procedures where each of them is characterised with initial information, action and output. These procedures represent on the one hand a systematic approach, on the other hand it will allow a solution which is appropriate to the level of protection required, meaning that they are also cost-effective. It was published in the VDI/VDE Guideline 2182 (VDI/VDE, 2007)

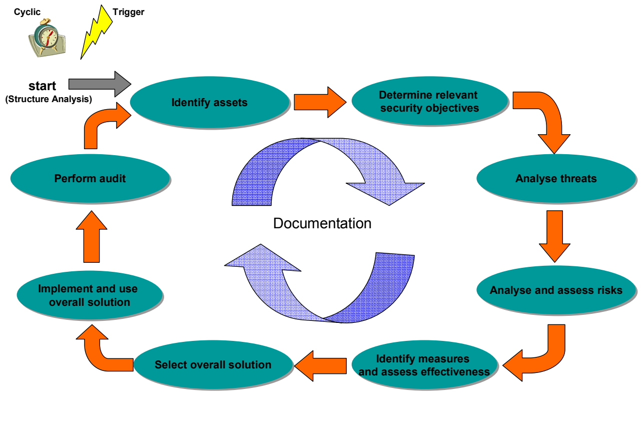

Fig. 1. Generic Procedure Model

2.2 Adaptation for VAN Project

Due to the fact that the VAN project uses these models for the first time, there was no real experience in using such procedures and the proposed auxiliaries like the excel sheet. It is a simple approach however many things are not fixed and therefore open. At first it was necessary to explain the model in detail and secondly to spread the 8 single procedures to the overall project work plan (only WP6 part). Furthermore, all the effort concerning the test and measurement was attached to the procedure "Perform Audit". Table 1 shows the allocation of the VAN IT-Security model to VAN task activities.

Table 1. IT-Security Model related to the VAN project related tasks

Task	Description of work	procedure according to the model
1	Status and Analysis Report on security mechanisms and security infrastructures	• No procedure
2	Definition of Security mechanisms in industrial environments addressed by VAN; Catalogue of attack scenarios	• Identify assets • Determine relevant security objectives • Analyse threats • Analyse & assess risks • Identify individual measures and assess their effectiveness
3	Service definition and protocol (functional) specification of a security layer	• Select overall solution
4	Security mechanisms prototype implementation	• Implement and use overall solution
5	Test report	• Perform audit

2.3 Expected Benefit

The use of the model was the beginning of a systematic approach in the VAN project especially in the working package 6 and therefore the major benefit. The partitioning of the 8 procedures to the existing project plan and particularly to the description of work was simple to realise and simple to explain to the project consortium.

Furthermore and contrary to the VAN project, the evaluation of the brand new procedure model and the corresponding VDI/VDE Guideline by using it within VAN project was a benefit for the GMA activities. VAN generates a list of comments and hints to the draft version of the guideline.

This opportunity was a great benefit for both sides. The VAN project can use a recognised model and the committee 5.22 "Security" in the GMA can improve it via external experts. The importance of the guideline can be easily defined, because the guideline will then be used as input to the IEC activities within the standardisation committee SC65C WG10 (in liaison with ISA SP99).

3. PREREQUISITES

Due to the fact that the overall topic security consists of several aspects such as operational, physical and communication security, the VAN project focuses only on communication security in industrial automation applications. Now all prerequisites with several aspects have to be defined. The model called this task a structuring analysis.

A structure analysis must be carried out before the procedure model is applied. This analysis includes a specification (as detailed as possible) of the IT-Security target and the corresponding assets on the one hand and a specification of the environment of use on the other.

3.1 *Specification of IT-Security Target and the Assets*

Fig. 2 depicts a VAN infrastructure example which is part of the description of the use case scenario commissioning (VAN consortium, 2006b). The commissioning is the step to set up a running virtual automation network, which includes the negotiation of the network setting for the devices and the transfer of configuration data from the engineering station to the VAN devices. The IT-Security Target will be bounded by the black line and is characterised by 2 interfaces. These interfaces are the connection to the outside world with a certain probability of threats and therefore only relevant for the consideration of possible IT-Security threats. Based on that IT-Security target and taking into account the given use case scenarios, it is now essential to define the assets and the relevant security objectives. For example VAN configuration data are the assets in these use cases and the IT-Security objectives are integrity and confidentiality.

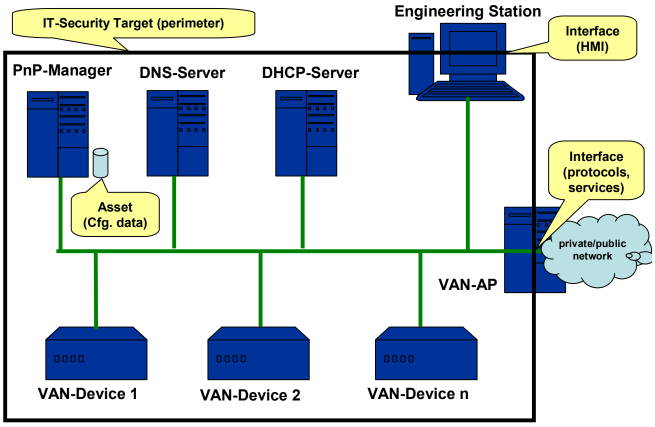

Fig. 2. IT-Security Target, Use Case Commissioning

3.2 *Specification of the Environment*

The specification of the environment of use concentrates for the most part on identifying influencing variables. These are characteristic values, relating to topography (building, environment), for example, which have a direct or indirect effect on the target of inspection. Examples of characteristics are: indoor/outdoor, exiting of a separated server room (looked), and are the communication cables/infrastructure devices hidden or directly accessible?

3.3 *Classification of IT-Security Threats*

Starting with the assembly of existing threat catalogs, the analysis of several well-known threats (only communication related) is necessary to extract the needed information for a threat classification approach. Therefore the following facts (VAN cons., 2006a) are relevant for the threat/risk analysis. It is missing in the procedure model and might be added.

The different kinds of attacks threaten the different objectives described in the first chapter. Independent of other kinds of classification, any security threat will try to breach the defence of one or more of the nominated objectives. So this kind of view considers the more technical aspects of the threats. The different forms of attacks can be assigned to these security objectives. In many cases, attacks threaten several objectives. Therefore they are classified into multiple categories which makes a unique classification not possible. Often, successful attacks open the chance for another threat (e.g. successful password cracking leads to a break of the confidentiality and integrity).

Table 2. Threats against security objectives

Threat against...	Kind of attack
authorisation	Pre-Attack Probe, Trojan Horse, Backdoor, Password cracking
availability	Denial of Service, SYN-Flood, Ping-Flood, Virus, Computer worm, Buffer overflow, Mailbombing, Message delay
confidentiality	Man in the middle, Trojan Horse, Sniffing
integrity	Buffer overflow, Message injection, Code injection
non-repudiation	Man in the middle, Message injection
third-party-protection	Backdoor, Message injection
authentication	IP Spoofing, Replay attack

Threats can be classified by the intention which is behind the attack. For every goal, a certain group of the security objectives are threatened. In order to defend a system against these threats, equivalent security goals can be defined.

Table 3. Goals of Threats

Threat reaches for...	Kind of attack
unauthorised information gain	Trojan Horse, Sniffig, Man in the middle, Backdoor (access), Password cracking (accesss)
unauthorised disruption of functionality	Denial of Service, SYN-Flood, Ping-Flood, Virus, Computer worm, Buffer overflow, Mailbombing, Message delay
unauthorised modification of information	Man in the middle, Trojan Horse, Message injection, Password cracking (access), Backdoor (access)
unauthorised fabrication of messages	Replay attack, Message injection

One way to classify threats is to sort them according to attributes of their threat agent. They can be described by their location, their intention or by the way they act towards the victim system.

Table 4. Threat agent characteristics

Threat agent characteristics	Kind of attack
origin is outside the system	every attack can be started from outside
origin is inside the system	Trojan Horse, Virus, Computer worm, Denial of Service, Ping-Flood, SYN-Flood, IP Spoofing, Buffer overflow, Message delay, Message injection, Code injection, Backdoor, Mailbombing
attack on purpose	every attack can be created on purpose
attack by accident	Denial of Service, SYN-Flood, Ping-Flood, Buffer overflow, Mailbombing, Message delay
active	Denial of Service, SYN-Flood, Ping-Flood, Virus, Computer worm,Trojan Horse, Buffer overflow, Mailbombing, Message delay, Message injection, Code injection, IP Spoofing, Backdoor
passive	Sniffing, Man in the middle, Trojan Horse

Depending on the area of the attacked devices and of the goal of an attack, a threat can have effects on different areas of a company.

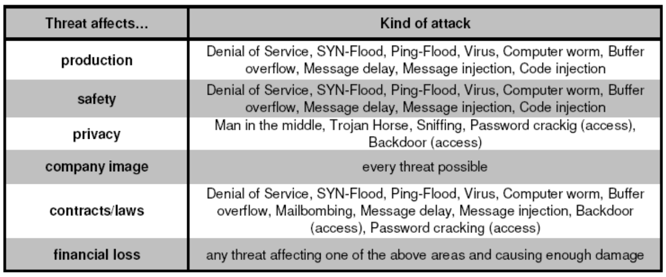

Table 5. Effects of threats

Threat affects...	Kind of attack
production	Denial of Service, SYN-Flood, Ping-Flood, Virus, Computer worm, Buffer overflow, Message delay, Message injection, Code injection
safety	Denial of Service, SYN-Flood, Ping-Flood, Virus, Computer worm, Buffer overflow, Message delay, Message injection, Code injection
privacy	Man in the middle, Trojan Horse, Sniffing, Password crackig (access), Backdoor (access)
company image	every threat possible
contracts/laws	Denial of Service, SYN-Flood, Ping-Flood, Virus, Computer worm, Buffer overflow, Mailbombing, Message delay, Message injection, Backdoor (access), Password cracking (access)
financial loss	any threat affecting one of the above areas and causing enough damage

4. VAN SPECIFIC REQUIREMENTS

Before the first procedure can be executed, VAN specific requirements must be considered. These are more or less functional requirements and requirements on IT-Security. Normally the definition of certain use case scenarios are helpful to identify the concrete requirements.

4.1 Requirements on IT-Security

Requirements that VAN have to consider are specific to IT-Security aspects of manufacturing and are related to use case scenarios and the corresponding infrastructure. The main use cases from the manufacturing industry point of view are: “Manufacturing plant with machine tools and supervisor”, “Distributed functions and data environment”, “GSM/GPRS remote monitoring system” and “Remote Internet maintenance”. Based on the analysis of these use cases, the following requirements were identified:

1) Identification of areas with the same level of security (category, isolation, connection management). These have already been dealt with in Chapter 4.

2) Access control for functions and users in a Client-Server architecture.

3) Mechanisms for testing the vulnerability level of a system or a sub-part (possibly in a dynamically adjustable way).

4) Mechanisms for attack prevention (from malware, viruses, etc.).

5) Mechanisms for attack identification and isolation.

6) Application of the “paranoid approach”, assuming that an attacker has internal knowledge of the system. This should cover all random events as well.

7) Network monitoring functions on connections (current and history log).

8) Integrity test functions.

9) Upgrade capabilities of communication interfaces, devices and computer systems (possibly with a management infrastructure).

4.2 Further Requirements and Limitations

There are 2 groups of further requirements. The first group is based on all the existing use cases which have influence to IT-Security. The second ones are related to the needs of industrial automation devices which are more or less embedded devices.

Security scalability: Security functions have to be scalable on devices and computing systems, according to the area of influence they belong to and primary functions they have to perform. Enable/disable of security functions may be possible on some exceptional occasions but it must be decided by security management. Scalability is important, considering limited resources of embedded devices. Described below are further requirements which Van has to consider:

All levels of the network must be protected from external attacks: The connection of the network with external WANs must be protected against any kind of attack (viruses, and so on). This means the platform must include mechanisms for the prevention, identification and isolation of attacks.

All levels of the network must be protected from intruders: Several levels of authorisation should restrict access to information stored on the network nodes. This will not allow unauthorised intruders to access data stored on PC hard disks.

Integrity test functions: Test for the verification of data integrity must be provided on a user’s request. So the user can verify the integrity of files after transmission from one computer to the other, but also due to memory faults.

Safe access for remote maintenance: Access for remote maintenance is allowed, however it is protected and restricted only to the relative devices which avoids interaction and conflicts with other system components.

Nowadays embedded devices increasingly permeate our lives. Unfortunately, security techniques developed for enterprise and desktop computing might not satisfy embedded application requirements. Another potential area of attack is physical access to security components. Security of embedded systems depends on the applications but failures of security mechanisms can result in physical side effects, including property damage or even personal injury. If you want to create a security embedded device you have to implant design security rules from the very start of your design. Attackers could exploit all possible ways to get the important information, decrypt data or gain direct access to control the compromised device. The next open issue of embedded systems is power management. Embedded devices often have significant energy constraints, and many of them are battery powered. By seeking to drain the battery, an attacker can cause system failure even when breaking into the system is impossible. This vulnerability is critical, for example, in battery-powered devices that use power-hungry wireless communication and can easily result in a DoS condition. Embedded systems are also highly cost sensitive. For this reason, most CPUs manufactured worldwide use 4-bit and 8-bit processors, which have limited space for security overhead. Many 8-bit microcontrollers, for example, can not store a big cryptographic key. This can make well established approaches from the enterprise world too expensive to be practical in embedded applications. Cutting corners on security to reduce hardware costs can give a competitor a market advantage for price-sensitive products, but it can also open back doors for potential attackers. The most important block of each embedded device which applies cryptography is a cryptographic processor. The quality of the cryptographic processor affects all other parts of an embedded device.

4.3 Legal Issues

One aspect of implementing security is to view these measures in the context of the actual contractual and legal environment. The algorithms used in order to protect communication channels are the very same as those used in human society to keep privacy/confidentiality, digital rights and digital signatures. Encryption technology has been regarded as a weapon material for quite a while and yet it still contradicts with the interests of various official institutions.

Special consideration applies in the case of a service contract with an infrastructure service provider. The most important issue is the fact that to keep data confidential, the service provider does not possess the knowledge whether a line breakage causes a security or safety problem. The information is fixed in the service level agreement, which may state a fine for exceeding certain predefined attribute limits (like the maximum length of a line breakage), however it does not forward the damage caused in this case to the service provider.

5. VAN TECHNICAL MEASURES

VAN as an integrated project not only aims at the conceptual and methodological aspects, it also targets the application and adaptation of technological means already established in the office domain. Hence the other field of work is dedicated to the evaluation and implementation of answers to the major security challenges encountered when transporting automation data via public networks. The following measures are relevant for VAN:

- The protection of the actual runtime data with special regard on maximum efficiency and determinism.
- The often less considered control data – the actual VAN traffic itself – is to be secured while keeping a maximum of flexibility of the chosen transport mechanism, Web Services.
- The active control of data entering the systems and devices on the runtime level by applying packet admission control and on the VAN Meta level introducing a sophisticated and distributed access control model.

5.1 Runtime Data Protection

The protocols used in automation networks are highly optimised for efficiency and emphasis is put on realtime behaviour namely the deterministic transmission of frames. Thus often (as in PROFINET IO) the communication is carried out on layer 2 preventing routing and hence the vanilla transfer via adjacent, probably public networks. In order to also address the security objectives referred to earlier, an encapsulation into a more secure transport channel is a consequential measure to protect the runtime traffic.

A classical means for secure data transport via unsecured networks is the use of encrypted virtual private networks. Here two major technological solutions can be considered. IPsec is the standard application schema when tunnelling is required. It is an integral part of the IPv6 implementation and has been implemented in several devices. However, for the transfer of layer 2 frames, the protocol has to be extended with L2TP (RFC 3193) This has been characterised by Bruce Schneier with the devastating comment “We strongly discourage the use of IPsec in its current form for protection of any kind of valuable information, and hope that future iterations of the design will be improved” (Ferguson et al., 2000), due to its uncontrollable complexity. VAN is striding to be the reliable set of measures to provide vendor independent interconnection between VAN devices and hence it was necessary to opt for a different approach.

The alternative has been found in the use of a transport layer security based tunnel technology called OpenVPN. Its use is widely spread, it has been ported to several platforms and it allows layer 2 and layer 3 transport respectively. The use of OpenVPN is also encouraged by the fact that it is provided as open source which allows descent evaluation and the opportunity to implement extensions if required. One of the challenges is the transport via several network segments which might not allow direct routing of IP traffic like the traversal of a demilitarised zone. Here a bastion host (a so called VAN Access Point) would be in charge of connecting two separate tunnels on the basis of strict security policies providing a transparent end to end channel. In the case of untrusted Access Points, a tunnel in tunnel strategy is foreseen which would ensure the integrity of the tunnelled traffic.

When providing technical means for automation use, the easy application in cooperation with the existing engineering tools and philosophies is a key requirement for success. Individual configuration is out of the question and the consistency of declarations on the communication path should not be borne by the engineering staff. Instead the configuration on a higher level is to be provided (task of the engineering workpackage in VAN) and the configuration and establishment of the tunnels is completely done via the VAN specific Web Services (VAN consortium, 2007).

This strategy allows for an abstract definition of a tunnel along a set of VAN Access Points, as the vast variety of options offered by OpenVPN could be drastically limited to a subset defined by the type of traffic to be transported and also by specification definitions.

5.2 VAN Communication Protection

As already mentioned the communication of VAN configuration, control and diagnostic data is carried out using Web Services utilising the advantages which already have been successfully implemented in B2B relations in the office domain. Web Services themselves do not provide any security means as such and rely on WS extensions and mechanisms of the transport protocol. One very basic method that is common to secure HTTP is to use the SSL variant which allows the integration of Public Key Infrastructures and hence provides the level of security nowadays commonly trusted in the ecommerce domain.

The Web Services employed in the VAN system according to the specifications carry a payload which is a completely separate XML file allowing for encryption and digital signatures applied individually by the different subsystems as they might be subject to vendor specific decisions and exchangeable format specifications. Hence the Web Service is terminated by a single process, the broker, which then distributes the inner XML file to the respective object based on object reference and method called.

The security measures in this section are therefore responsible for transporting this respective Web Service to the intended end point, while at the same time preventing eavesdropping and man in the middle attacks with all cryptographic methods known and applicable today.

5.3 Access Control to VAN System

The check as to which traffic is allowed to enter a system is one of the primary tasks of a security solution being employed anywhere. VAN thin specifically includes the management of Ethernet frames on the runtime channel as well as – and more general – the control as to which Web Services should be acceptable.

The check on Ethernet frame/IP packet level, which frames or packets are allowed, is to be applied mainly at the tunnel endpoints. The intended final implementation does bear the fieldbus stack and the VAN stack in the device where the fieldbus communication is bound to the virtual interface provided by the tunnel. These interfaces are then chosen to be addressed by link local addresses as they only would connect single device instances end to end. Thus no filtering is necessary. However the project is of course aware that not all future devices will be VAN enabled and hence the physical separation of an automation application bearing device and tunnel ingress has to be considered as an option. The specific filters are investigated and the implementation options for hardware support are specifically considered in the security workpackage (together with the realtime workpackage).

The burden on the actual access control instance for VAN specific communication is even higher. Access control in the sense of VAN is the evaluation of every Web Service for authentication and authorisation to enter a specific device. This also includes the handshaking to establish a tunnel which implies a tunnel to be trustworthy as a cable connection after the ACL has allowed the tunnel setup messages. As Web Service relaying (internally called routing but contrary to the standard by the same name) may be used to reach not directly addressable nodes in other networks, a relaying device, mainly a VAN Access Point, may have to locally terminate a Web Service and decide if relaying is allowed. In both cases (local resource addressed or message to be relayed), the Web Service request data is given to a separate Policy Decision Point (PEP PDP separation as usual) where the locally stored policy is consulted if the respective request is to be allowed, denied or dropped. This is provided to the enforcement point where the broker acts accordingly.

This check is deliberately performed in every instance of the communication path, effectively applying the defence in depth principle widely accepted in security applications. In Fig. 3 the red bars illustrate all effective checkpoints where a message has to pass to be successfully delivered to the destination VAN device (VAN consortium, 2006b).

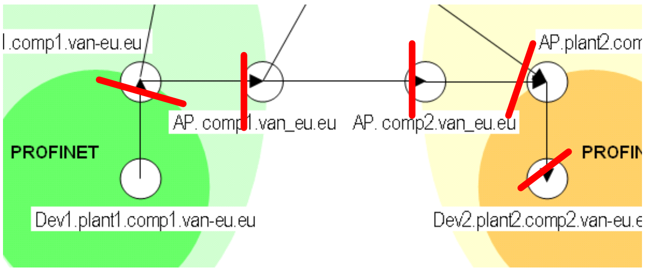

Fig. 3. Visualisation of the defence in depth principle

The use of the above mentioned principles is expected to be a package of measures fulfilling the requirements collected during the project and continually identified in the security model presented before. The technical means do of course not guarantee 100% security but allow a modular replacement of insecure methods and protocols by those where security measures can be applied in a scalable way from embedded to high performance platforms.

6. REFERENCES

Ferguson, N. and B. Schneier (2000). *A Cryptographic Evaluation of IPsec*, Tech. Report, Counterpane Internet Security, Inc., 3031 Tisch Way, Suite 100PE, San Jose, CA 95128.

VAN consortium (2006a). *Deliverable D06.1-1 Status and analysis report on security mechanisms and security infrastructures*.

VAN consortium (2006b). *Deliverable D06.2-1 Security mechanisms for automation*, Draft Version.

VAN consortium (2007). *Deliverable D02.2-3 TechPCC-Platform Overview*, Draft Version.

VDI/VDE (2007). *Informationssicherheit in der industriellen Automation - Allgemeines Vorgehensmodell*, Richtlinie 2182, Entwurf.