Design of a Telematics System for Saab Giraffe AMB

Master of Science Thesis in the Master Degree Programme, Embedded Electronic System Design

Mathias Lundell
Johan Rubenson

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
Göteborg, Sweden, June 2012

Design of a Telematics System for Saab Giraffe AMB
MATHIAS LUNDELL
JOHAN RUBENSON

Examiner: Per Larsson-Edefors

Department of Computer Science & Engineering
Chalmers University of Technology
SE-412 96 Gothenburg
Sweden
Telephone + 46 (0)31-772 1000

Department of Computer Science and Engineering
Gothenburg, Sweden June 2012

Abstract

Telematics is a technology that is not widely spread in the defense industry. This master thesis report presents some of the criteria that must be fulfilled in order to introduce a wireless unit that communicates via GSM in a radar station from Saab Electronics Defence. The wireless unit is designed as a diagnostics tool called the Saab Telematics Unit (STU). It is running on an embedded Linux platform from Host Mobility and communicates with Saab's computers via Ethernet. All information is presented in a .NET web platform together with a MySQL database and a standard file server.

The master thesis shows that the industry has been skeptical to wireless solutions due to security risks, like hijacking of the radar via the wireless connection. Countermeasures, for example encryption and VPN-tunneling, can be used to minimize those risks. It is important that an intelligent choice of what is sent over the air is done, so that a security breach does not result in company or military secret information being leaked. The main guidelines that should be followed to guarantee that it follows Saab's security standards are traceability, information security and disaster recovery. Traceability is the ability to see who has done what. Information security is for example authentication, authorization, encryption, etc. Disaster recovery is a plan of what to do if classified information is leaked or if the system is somehow compromised. As these security concerns have been addressed, the skepticism from employees at Saab has been reduced. They have more and more begun to see the benefits of telematics and that it can be a secure technology.

Acknowledgements

Designing software and choosing hardware for a telematics solution is not a particularly difficult task. The difficult part is to customize it to fit with the customer’s needs. The customer in this case is Saab Electronics Defence and their particular need is a solution that maintains a high degree of information security. It has been a learning experience for both of us to go the whole way from planning to a working prototype that has CORBA, SSH, SFTP, encryption, database connectivity and a myriad of other features.

All this would not have been possible without the aid of the engineers at Saab Electronics Defence and Consat AB. We want to particularly thank Peter Lidman at Saab for the endless hours he spent with us in the lab, fine-tuning the prototype. We would also like to thank Anders Martinsson at Saab for his optimistic attitude and enthusiasm, without his assistance we would not have been able to do this project. Stefan Engström at Consat AB was the one who brought us the idea in the first place and contacted us with Saab. He has been important in the design process, always introducing new ideas and interesting perspectives.

Finally we would like to thank professor Per Larsson-Edefors from Chalmers University of Technology who has been guiding us through the practicalities of the master’s thesis and helped us with the report.

Gothenburg, 2012
Mathias Lundell & Johan Rubenson

Table of contents

List of Figures

Abbreviations

AES – Advanced Encryption Standard
CAN – Controller Area Network
CHAP – Challenge-Handshake Authentication Protocol
CORBA – Common Object Request Broker Architechture
CPU – Central Processing Unit
DES – Data Encryption Standard
FIPS – Federal Information Processing Standard
FMV – Försvarets Materielverk
FTP – File Transfer Protocol
GAMB – Giraffe AMB
GPRS – General Packet Radio Service
GPS – Global Positioning System
GSM – Global System for Mobile Communications
IDL – Interface Definition Language
IMT – International Mobile Telecommuncations
IP – Internet Protocol
IP-Core – Intellectual Property-Core
MUST – Militära Underrättelsetjänsten
NSA – National Security Agency
OMG – Object Management Group
ORB – Object Request Broker
PAP – Password Authentication Protocol
PPPD – Point-to-Point Protocol Daemon
RAD – Rapid Application Development
SCP – Secure Copy
SFTP – SSH File Transfer Procotol
SQL – Structured Query Language
SSH – Secure Shell
STU – Saab Telematics Unit
TCP – Transmission Control Protocol
USB – Universal Serial Bus
VPN – Virtual Private Network
WLAN – Wireless Local Area Network

1 Introduction

Fault tracing is something that all products sooner or later will have to go through. Almost all technology is built up by complex systems and finding faults may be difficult or almost impossible without specialized diagnostic tools. If no such tools exist, the only option may be to replace every part of the system until the error disappears. This is in most cases not a feasible option. This section will present a background to why telematics is a growing technology that is used in an increased number of business areas. It will also explain the purpose and boundaries for this master thesis.

1.1 Background

The development of integrated circuits has not only changed how our generation lives and socializes, it has also changed the rules for warfare and defense industries. Information has throughout history played a very important role in almost all military conflicts. Without the aid of the telegraph, the British Empire would not have been able to subdue the Indian revolts during the imperialism (Misa, 2004). Technology today has evolved enough for an army to gather information without even sending people near the enemy. Instead of scouts there are radars, instead of fighter pilots there are unmanned aircrafts. One talks about the digital battlefield (Tode, 1998).

Saab's products ensure awareness of the air situation around a chosen area to be able to detect, localize and identify threats before they become dangerous. This type of information, together with other defensive resources, gives a more secure environment for people on the ground in that area (Tode, 1998).

If there is a system fault and parts of the system don´t work correctly, the resulting lack of information can be catastrophic. The customers are located around the world and need to solve faults and service issues with short lead times as a functional radar may be a matter of life and death.

As the integrated circuits have evolved, the expenses for systems using wireless communication, among others, have dropped. The price change and a wider use of the technology have not only spread the wireless networks around the planet, it has also started to be used in applications where machines communicate with each other. For instance, a vending machine can be connected to an inventory system and automatically place orders when certain items run out. This is also called Machine-to-machine (Machine-to-machine, 2012). Wireless communication also opens up the possibility to read out information such as diagnostic status. That knowledge can for example be used to better plan and implement preventive maintenance. It also increases the customer and market value of the product. The new functionality can also be used as a service-based product to the aftermarket.

1.2 Purpose

Saab's radar systems are used to detect, locate and protect against threats, such as incoming grenades. Both military and civilian applications involving control of the airspace may be desirable. The purpose of this study is to, in collaboration with Consat Engineering AB, develop a proof of concept for a diagnostics system for Saab Electronic Defence's radar products Arthur and Giraffe AMB (GAMB). This diagnostic system, known as the Saab Telematics Unit (STU), should allow for troubleshooting and status monitoring of equipment remotely.

Since telematics is an unexplored and new technology for defense industry, some different use cases will be presented in this report. These will act as a motivation for introducing this technology at Saab.

One reason that telematics hasn’t been introduced in the defense industry earlier is the possible security threats. There are fears that this technology would compromise the security and in some way give the enemies an advantage. A short study of what criteria must be fulfilled and what obstacles must be overcome in order to introduce a secure solution for telematics at Saab is part of the purpose for this master thesis.

1.3 Boundaries

To construct a specialized hardware solution would be possible but would require too much time. Only commercial hardware platforms will be used, no hardware will be designed in this master thesis. The main reason for this is to give the project a jump start.

It is possible to measure, for example, memory and processor usage and try to minimize it. In order to guarantee the correctness of the software, special software analyzing programs can be used. However, no exact measurement of the software’s performance will be conducted. The reason for this is that the time performing software verification could be better spent elsewhere. If Saab is going to make a product of the STU, they will want to rewrite the software themselves so they are sure that it follows their standards. The STU will be developed with the intention of having one STU per radar station, but no testing with multiple radar stations will be done.

The STU will be using a GSM connection to connect to the internet. The STU will not be restricted to this technology. The GSM connection should only act as an example of a possible technology for transportation of information. The connection can easily be changed to another technology that is available and suitable for a particular customer’s solution. It is possible to connect to the internet with other technologies, for example the information could be sent via a satellite connection or a fiber optic connection. The GSM solution is used as an example because it is the most frequently used connection type for telematics solutions.

The presentation of the data that the STU transmits has a lower priority than the rest of the master thesis and thus only a simple web site that shows some basic functionality will be developed. It will have a basic user account feature for log in, but no traceability and advanced authentication features. No work will be done on the design of this web site. It will use a standard design template from Microsoft Visual Studio 2010 without modifications. The design is something that must be based on how the users are going to use this system. This is not something that could be done before we know what the system can do and who is going to use it. The focus with the web site is to show what can be done in terms of key features.

There are a number of ways to collect data from an advanced product like a mobile radar station. Besides the radar computers it is possible to connect and retrieve information from the diesel generator, the truck and external sensors, for example gyroscopes and accelerometers. The lab at Saab that is accessible for testing has a cluster of radar computers, called the DEM computers, which are open for communication over Ethernet. The DEM computers are computers in the radar stations that run Linux and handle the connection to the radar hardware. They contain so much important information that is interesting for both engineers and customers that the STU in this first phase focuses solely on retrieving information from them. Later on other information channels can be implemented.

2 Theory

This section contains a short briefing about the different technologies that have been used in this project. The technologies are presented to create a better understanding of the implementation section, where all these components are used to create a bigger system. Many of these components have numerous functions and possibilities, a selection of the most important and useful components for this master thesis will be mentioned.

2.1 Embedded Linux

Embedded Linux is operating systems based on modified Linux kernels. The reason for creating a modified version of the Linux kernel is to relax the performance needed to run the system. There are several advantages to be able to run an operating system like Linux on a low performance platform. One of the main advantages is the built in support for network and peripheral units.

Examples of embedded Linux operating systems are Android and MeeGo. Embedded Linux is thus not an operating system per se, as is commonly believed, but a name for Linux running on embedded systems. Depending on the type of product, different operating systems are suitable. One of the main competitors that works on various hardware platforms is Windows Embedded Compact which is Microsoft´s response with a stripped down version of their Windows platform.

One major advantage with Linux based platforms is that new IP-cores and new protocols are developed faster than for proprietary operating systems like Windows. This depends mostly on the demand and contribution from the large user base and the simplicity of developing drivers and software modules. The modular design of the kernel gives the possibility to either compile the driver modules together with the kernel, or add them during runtime.

These advantages together makes it easy to configure and use embedded Linux for most platforms. The large community and the fact that it is open source makes it easy to find information on how to tailor the system to specific needs. Licensing fees and restrictions are also no problem since it is open source, provided that purchasers are not prohibited from redistributing the open source components.

The most important disadvantage of a system based on a Linux kernel is if a code error occurs in the kernel space, the complete operating system can crash. This is not a major problem since most programs only need to run in the more fault tolerant, but more restrictive, user space. But to achieve real-time operation with hardware interrupt handling, the code has to be executed in kernel mode. If the executed code isn´t correctly written the system can be unstable and create problems (Addison, 2001).

2.2 Common Object Request Broker Architecture (CORBA)

CORBA is used in the GAMB as an information transport backbone between different system nodes. One of the reasons for using CORBA is the platform and language implementation independency. A brief description of what CORBA is and consists of is given in this section.

2.2.1 Overview

Common Object Request Broker Architecture (CORBA) is an open technical standard. It specifies a system that allows a user to request services from objects that are running on other machines and use them as if they were local objects (McHale, 2007). The program calling the remote object has no knowledge of where the object is implemented. CORBA acts as a middleware and takes care of all those details. This kind of system is also called a component technology (Lewandowski, 2008).

The idea of a component technology is that components should be interchangeable as long as they provide the same interface. As an example, you have created a component that calculates salaries. After a while you realize that you have to take in consideration of how much overtime an employee has done. So you write another component with the same interface as the first. Since they have the same interface, you can just swap them, and other programs that are using the old component will automatically work with the new one.

So CORBA does two things, it maintains components and their interfaces and locates these components. Other examples of middleware packages are Distributed Component Object Model, Java Remote Method Invocation, IBM MQ Series, Microsoft's COM and .NET (McHale, 2007).

Some strengths of CORBA are

- Mature technology
- Object oriented
- Distributed system
- Independent of operating system
- Independent of processor architecture
- Implemented for many programming languages, i.e. C/C++, Pascal, Ada
- Efficient – data transmitted in binary format, low bandwidth necessary
- Scalable – adopts well to large amount of communication data and many connections

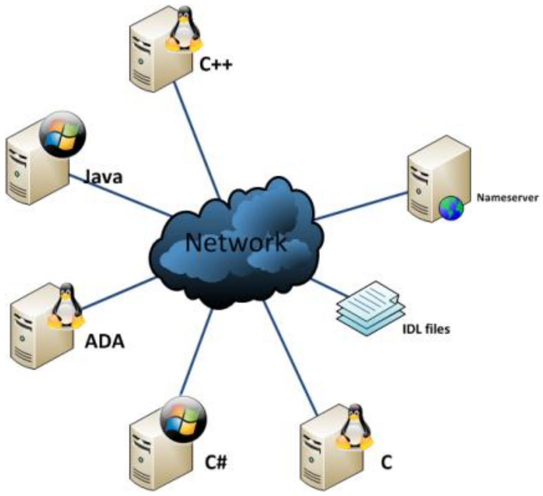


Figure 1. Clients/servers connected with CORBA

2.2.2 Object Management Group (OMG)

The Object Management Group is the industry consortium that provides the CORBA specifications. It is a non-profit free membership organization with the mission "to develop enterprise integration standards that provide real-world value". Another standard they maintain is the Unified Modeling Language (OMG, 2012).

2.2.3 CORBA implementations

There exist many different CORBA implementations, both commercial and open source. Some of the most common are:

- omniORB
- JavaORB
- ORBacus
- PyORB

The differences between the implementations are mainly licensing options, programming language bindings, performance and platform support. There is no guarantee that the different implementations are compatible. It is important to study in detail which version of the CORBA specification they support, and also how they have chosen to implement it.

Since Saab has chosen to use the open source solution omniORB, the focus for the rest of the report will be on that specific CORBA implementation.

2.2.4 Interface Definition Language (IDL)

CORBA interfaces are independent from implementation languages, such as C/C++ and Java. In order to specify the interfaces, another programming language called Interface Definition Language (IDL) is used. With this it's possible to define objects, their methods and members. The IDL file is then compiled, using a tool provided by the specific CORBA implementation, into an implementation specific file. If you are writing your program in C++ you will get a header and source file upon IDL compilation. The omniORB IDL compiler is named omniidl. If two different compilers, following the same CORBA specification, compile the same IDL file, the resulting programming language mapping should also be the same.

2.2.5 CORBA Name Service

The objects of a CORBA system are usually located using naming contexts. They can be described as named nodes that have objects bound to them. These bound objects may also have specific names. The naming contexts can also be bound to other contexts and thus creating a relational naming graph. This graph is usually, but not necessarily, a tree hierarchy (OMG, 2004), (OmniORB, 2008).

The naming service of omniORB is called omniNames. It is a service that takes a human-readable name as input and returns a reference to the associated object (Grisby, 2008). Each omniORB instance must have a reference to the root context of the naming service. The reference to the root context is usually read from a configuration file called omniORB.cfg. omniNames can be run on any computer on the network as long as it's reachable and the clients have the correct reference (OmniORB, 2008).

A client that wishes to use an object references a specific naming context and resolves the name of the object. To resolve a name is to get the object with that name from the naming context (OMG, 2004).

2.3 Secure Shell (SSH)

Secure Shell is a protocol used for connecting clients to a server environment over an encrypted line through a local network or internet (Ylonen, 1996).It was designed as a replacement to Telnet and other insecure remote protocols. There are currently two major versions available, SSH-1 and SSH-2 (Secure Shell, 2012).The latter is considered more secure and has more features.

SSH is used to provide secure remote login, file transfers, port tunneling/forwarding, etc. The CPU overhead for encryption is negligible on a standard PC (Ylonen, 1996). Many different implementations of SSH exists with various licensing options, both proprietary and open source.

2.4 SSH File Transfer Protocol (SFTP)

This is an extension to the Secure Shell protocol (SSH) that provides file transfer mechanisms. The main advantage above regular file transfer protocol (FTP) is that the file transfer can utilize the authentication and security features of SSH (SSH File Transfer Protocol, 2012). Sometimes this protocol is thought to be FTP with security principles, but it is in fact not based on FTP at all. SFTP is a successor to SCP with the benefit of resumable file transfers among others.

2.5 Secure Copy (SCP)

Secure copy is a protocol for file transfer between network nodes. It uses an SSH tunnel to securely copy files between computer nodes with an encrypted connection (Secure copy, 2012).SCP uses TCP port 22 by default.

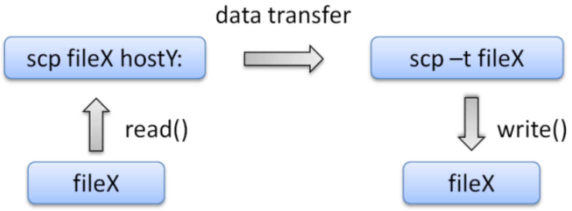


Figure 2. File transfer from hostX to hostY (Pechanec, 2007)

2.6 Point-to-Point Protocol Daemon (PPPD)

This program is used to establish a point-to-point protocol connection. The connection is usually over IP, but other network protocols may be used as well. PPPD provides authentication and manages IP addresses. Examples of supported authentication protocols are CHAP and PAP (Mackerras, 2012).

When a link is supposed to be set up using a modem, it is useful to use scripts that prepare the connection. The program called chat can be used to communicate with the modem to set access point name and other settings necessary before the link can be established (Kirch & Dawson, 2000).

2.7 MySQL

MySQL is a very commonly used open source relational database management systems (MySQL, 2012). It is popular in both commercial and open source projects partly due to the many edition and licensing options available. One of the main strengths is the versatility. It is possible to run on most operating systems and there exist APIs and libraries for many programming languages. It is possible to connect to a MySQL server in C using the MySQL Connector/C. Similar connectors exists for C++, Java, etc. Another strength is the extensive documentation available.

2.8 Telecommunication

Telecommunication is a method for transferring information over a significant distance. The most known type today is the GSM network, which is the second generation of wireless communication systems.

2.9 General Packet Radio Service (GPRS)

The GPRS, General Packet Radio Services, technology is a platform for mobile data in the GSM network. With GPRS your connection to internet is always open and the data is transferred in packages when needed. This makes is possible to use the phone for voice communication at the same time as data transfer.

Another big difference with GPRS, compared to regular voice traffic, is that the fee depends on the amount of data that is transferred and not connection time. This has created a possibility to have equipment always connected to a low fee. This technology has been available in Sweden since year 2000, but became broadly used in 2002. The technology offers a transfer speed of 30-100 Kbps. As the use and demand has increased, the modems are today cheap and widely available (General Packet Radio Service, 2012).

2.10 3rd Generation Mobile Telecommunications (3G)

New services, like video calls, require faster internet connection than the GSM data services can provide. Therefore a new generation of wireless standards, 3G, was introduced. The 3G communication system is often denoted as a technology, it is in fact a generation of standards that fulfil the International Mobile Telecommunications-2000 (IMT-2000) specifications.

The transfer rates available for 3G, specified by IMT-2000, is between 144 Kbps and 2 Mbps. Since 3G mainly is aimed towards voice communication, several 3G extension standards for data transfer have been developed. One of the most common is HSDPA, which supports both data and voice traffic and has peak rates of 14.4 Mbps and average rates of 400-700 Kbps (Valenzuela, 2007).

2.11 Advanced Encryption Standard (AES)

After five years of evaluation the American National Institute of Standards and Technology announced AES as a federal information processing standard in November 2001. During that time several different designs were evaluated before AES was deemed most suitable (Advanced Encryption Standard, 2012).

AES is based on the Rijndael encryption algorithm, which is a symmetric block cipher, and was intended to be the successor of DES (Xunhua, Coppersmith, Matyas, & Meyer, 2008). The algorithm was invented by Joan Daemen and Vincent Rijmen. AES uses 128-bit data block size and cipher keys that are 128, 192 or 256 bits long. Depending on the size of the key, the encryption is called AES-128, AES-196 or AES-256.

Different modes of operation exist for most cipher algorithms. With the mode chained block encryption the cipher is not only dependent on the key and the block data, but it also depends on the results from the previous blocks (Block cipher modes of operation, 2012). For the first block a so called initialization vector (IV) is used. Thereafter the result from the first block is fed to the next block. This prevents that if one block is cracked, the whole message is compromised.

The academic definition of breaking a cipher is: “finding a weakness in the cipher that can be exploited with a complexity less than brute-force” (Schneier, 2000).This definition of a break doesn’t take into account if it is computationally practical, just that the cipher has weaknesses. It is possible to break AES, and a method to do so was presented in 2011 (Bogdanov, Khoratovich, & Rechberger, 2011). The authors managed a first key recovery attack on AES-128 with the computational complexity $2^{126.1}$and for AES-256 $2^{254.4}$. Previous known attacks have mainly been side-channel and related-key attacks (Advanced Encryption Standard, 2012). The conclusion is that the “attacks are of high computational complexity, they do not threaten the practical use of AES in any way” (Bogdanov, Khoratovich, & Rechberger, 2011).

A national policy from the National Security Agency (NSA) states that AES could be used to, not only secure sensitive (unclassified) data, but also classified (CNSS, 2003).

“The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths.”

3 Method

The software development process that has been used resembles the Rapid Application Development (RAD). RAD contains a quick pre-planning process before the construction process is started. The planning is continued during the project and customers can actively see the current results and steer the project in the wanted direction. This allows the project to be carried out rapidly while still making it possible to adopt changing requirements. By having regular meetings with the customer, a survey and current status presentations, they have been able to share their want and needs. The product's implementation and features have changed accordingly (Gottesdiener, 1995).

The reason for using RAD was that the customer, Saab, was unsure of what features were possible to implement and who the end user was going to be. Using RAD made it possible to quickly show them a first prototype and thereafter shape the product as they wanted.

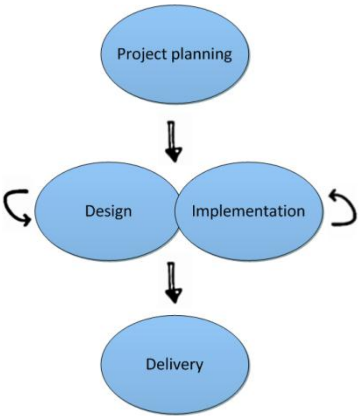


Figure 3. RAD work flow

To utilize the RAD model there were three opportunities offered to a chosen group of developers at Saab to evaluate the designs and features implemented at different periods of the project. With the key requirements in mind, a survey was created to investigate what features the developers thought were the most important and useful.

There were also two presentations where solutions and features were presented to get feedback of the usefulness and to create a discussion about which direction the future development should take. These presentations, especially the first were used to reply to the first feedback and feature discussion from the survey. Following up and developing features based on feedback from people that work with the equipment makes the end product more adapted to the user's demands.

To get a good approach against security issues during the development process, a meeting with the chief of IT security at Saab was held. He pointed out the main concerns: traceability, information security and disaster recovery. More information about these can be found in section 5.5.1 Saab security .

4 Resources

The Saab Telematics Unit (STU) uses a prototype of the hardware platform MX-4 from Host Mobility, which runs an embedded Linux platform and has a GSM/GPRS modem for wireless connectivity. Ethernet is used to connect the STU to Saab's computer systems. MX-4 has an ARMv5 processor from Toradex that is powerful enough to power graphical interfaces, which could be an option in the future. The programs used on it were cross-compiled with a tool chain provided by Host Mobility (currently available at: http://www.hostmobility.org/repo/elito/FC10/). All programming was done in Eclipse CDT, running on the Linux-based operating system Fedora 16.

Saab's laboratory computer system consisted of a Linux server, called DEM, with all company and military secret information removed. It is one of the standard platforms that are used in both Arthur and Giraffe AMB, which are two of Saab's main radar products. The only significant application running on the platform was a customized error handling package.

PPPD, together with chat scripts, was used to setup a GSM/GPRS link.

The following are programs/libraries that are used in the main application:

- Botan-1.10.1
- omniORB-4.1.6
- Libssh2-1.4.0
- MySQL Connector/C
- OpenSSL
- SCP
- SFTP

5 System implementation

Almost all systems today are built from modules. The reason for using module-based implementations is that they are easy to adapt. Future projects can reuse some modules and remove others. Different modules can be created by different companies. Therefore are faults often very hard to solve without any diagnostic data available. The barrier for a quick and easy fix of the faults is in many cases the availability of the hardware. The hardware, that for example could be a vehicle, has to be taken to a special facility where the diagnostic equipment is available or a technician has to get to the hardware with the diagnostic equipment (Salman, 2011). Both approaches are widely used and work great, but they are in many cases not time efficient methods. On systems that have a more critical field of use, a minimizing of the time disposal for solving faults could be desirable. Telematics is a technique that could be used to minimize the time disposal by shortening the time to get the diagnostic data.

Telematics is a word that involves remote communication and information. A typical telematics solution is Global Positioning System (GPS) integrated with mobile communications technology in navigation systems. Over time, more and more advanced areas of usage have evolved. Some of them are: stolen vehicle tracking, theft notification, remote heater start, emergency call with automatic positioning information (WirelessCar, 2012). Even companies that operate in traditionally more conservative lines of business, like military, are beginning to see the benefits of remote access to vehicles.

The traditional way to read diagnostics from a vehicle is to store the information locally and later connect it to a computer and read the data. This has one major advantage, reliability. It is very unlikely that the data will be corrupt or lost. The downside is that the time between event and read could be too long and an equipment to read out the data has to be connected.

Another way to use the diagnostic data could be that the system has an on-board diagnostic system with a telematics unit to transfer all data to a backend system for later analysis. Then the data could always be ready for analysis of a technician. The downside with this approach is that there will be a cost increase to transmit data wireless and there will also be a risk of losing data due to bad reception or other problems with the connection. If there is a possibility to use a local storage together with a telematics unit, then the advantages from both options are fully utilized. The negative aspects are increased complexity and cost.

5.1 Communication

GPRS and 3G are today technologies that are very straightforward and easy to use. But when talking about military equipment, there are situations where wireless telecommunications systems like GPRS and 3G don’t exist or could be damaged. It is hard to predict what can happen in a war situation and therefore different communication solutions should be discussed.

Signal modulation is a technology that has been extensively used around the world for sending information through an analog signal path like telephone lines. It can, as an example, be used to connect computers to internet, e.g. ADSL (Chen, 2001).This is a simple and cheap solution that is applicable to almost all analog communication systems.

Another option is to install a fiber cable between the points where a communication is desired. This cable can be used to transfer all information and when it is finished it can be removed. The cable can be used as a gateway or extension to other networks that are far away, for example, a fiber cable connected to a radar station in one end and to a nearby telephone network in the other.

Instead of fiber cables, directed antennas for WLAN or radio modules can be used. They provide a fairly short communication range, around 100 m to 5 km is common but longer range is possible. This solution is quite easy to deploy but there may be questions about security since information may be intercepted. With enough encryption and other defensive measures, that should not be a problem.

If there are no telephone lines or GSM networks available, a satellite connection may provide the best solution. It is not dependent on a country's infrastructure and provides connection speeds of about 500 Kbps (Satellite Internet access, 2012).

The downside with having internet access via satellite is the price. It is very expensive to send and receive data and the modems are also expensive. Still, the benefits may make it affordable.

5.2 Hardware platform

Telematics is not an unusual business area today. There are many companies that develop different platforms with many different applications, but most adhere to automotive or industrial standards. There are few companies that demand a telematics solution with hardware that conforms to military standards. Therefore there is a need to develop a specialized solution with a heavy duty cased hardware that is adapted to the application and nothing more. A specialized solution may be the best choice in cases where it is difficult to find commercial products that meet the requirements.

In one way, to have several possible hardware choices is good, but off-the-shelf products often come with redundant components and features. Any functionality that isn't needed can cause problems with the main application, add to cost and take more space. Even though most of the extra features on these available platforms can be turned off, there is still an ambition to choose a platform with as low complexity as possible for the current application. Still, there has to be room left for future changes of the application and its implementation. The military applications is in this case a low scale production, not many products ship every year (<100). Due to this fact, it is not cost effective to develop a dedicated hardware platform in this case.

One reason to do the opposite, and develop a dedicated platform is to have control of the development process and minimize the cost in a full scale production. But this would have been more of interest if the current application, diagnostics, had supported some critical process for the main application, the radar system. A few of the most interesting hardware platforms that have been considered for this project are presented in the subsections below.

5.2.1 In-house hardware, Advanced Information Centre (AIC)

The AIC unit is a platform that is developed by one of Consat´s affiliate companies. It is developed for the automotive industry and has many features. The hardware is built around the MCP5200 microcontroller from Freescale. This microcontroller was released in the year 2005 and Freescale guarantees production until 2020. The unit has the connections and telematics modules needed but also many extra features that are unnecessary. For example it has outputs for a graphical interface (Freescale Semiconductor, 2012).

5.2.2 Host Mobility, MX-4

A Swedish company, Host Mobility, is working with telematics platforms for many different industries. They are developing a new platform named MX-4 that is an update on the old MX-3 that has been widely used in the automotive industry. The MX-4 is still on the drawing board and therefore it was only possible to get a prototype unit for this platform. The benefit of this is that there is a possibility to change the end product. Another advantage of this product is that the processor module is mounted on a separate board, and therefore an upgrade or exchange of the processor board really simple. The processor board is supplied by an external partner, named Toradex that has processor boards in a variety of performance alternatives. All the processor boards are based on the ARM architecture that is widely spread in the hardware industry (Host Mobility, 2012).

The platform also supports the interfaces that are necessary to be able to connect the equipment to Saab's systems. In addition, the platform also has inputs and outputs for future features, for example temperature probes.

5.2.3 Saab DEM

The Saab system consists of multiple computer nodes that run different parts of the system. These nodes are running standard Linux platforms that are adapted to run a critical system which by no means may fail. By integrating the telematics application together with the DEM computers, the only external hardware necessary is for the wireless communications. Instead of always running the telematics application, and thus risk causing interference with the core applications, it may be better to only start it in service situations. An antenna and a modem for the wireless communications could be always connected to the computers or only connected during service situations. This implementation the customers will have control over the system when the telematics is active and that could increase their trust in this product. Because only an antenna and a modem have to be added, this would definitely be the cheapest solution.

The disadvantage with running the diagnostics from the same hardware as the system is that the service issue could involve the node that the diagnostics running from. In some cases the issue could be of a severely level that the node that should run the diagnostics is faulty. This results in that no trace faulting can be done by the diagnostic tool and thereby a manual diagnostic has to be done on site.

5.2.4 Standard PC

It is possible to use a standard computer to handle the tasks of this system. A standard computer will have all necessary connections to implement a communication with the Saab system and also have the possibility to easily connect telematics modules, like a GSM modem.

The advantages of a standard PC are good performance, an easy solution both in terms of implementation and integration, and no special equipment needed. Standard PCs are always available for purchase. The disadvantages are that there would be a lot of features on the computer that wouldn't be needed and thereby create more fault possibilities. A standard PC would not be cheap to get sturdy enough to be used in a hazardous environment like this. In other words, an already rugged customized PC would have to be purchased.

5.2.5 Microcontroller

A solution based on a real-time OS running at a 32-bits microcontroller will be a really cheap hardware solution. For example a Microchip PIC32 microcontroller could be used. An embedded solution has cheaper hardware, takes less space and is more power efficient than many of the other solutions.

The problem is that it takes many hours of software development before a microcontroller without Linux has the same functions like a Linux environment. Therefore the software will be a very complex solution.

5.2.6 Smartphone

The performance of smartphones has increased significantly these last years. Many models have processors with performance comparable to standard computers. This performance together with all telematics equipment already built in makes the smartphone an interesting platform for telematics systems. The problem in this situation is the problems with getting phone hardware sturdy enough to be used and mounted in a hazardous environment.

5.3 Hardware decision

The decision of hardware was mostly based on performance and stability issues. An embedded Linux platform was chosen because it is powerful but has low system requirements. This decision is also a direction towards flexibility and modular design of the software solution. The goal is thereby that the software not will be dependent of the hardware platform.

The plan was to make the software run on any standard hardware without doing a massive makeover of the software. As the software doesn´t use any special hardware aside a standard Ethernet and USB connection, most of the hardware choices, except the smartphone, were possible.

A reason for using an embedded solution compared to, for example, a standard PC is that the power consumption is significantly lower. The Giraffe AMB has a diesel generator that powers its computers. If new equipment is going to be introduced, it is necessary that it doesn’t overload the generator. The power consumed also affects the rate of which the diesel tank is depleted. It is also possible for embedded hardware to run on a battery if the power consumption is low enough.

5.4 Software platform

The design process of the software has been aimed towards a module-based solution. Each feature of the software could run individually without any other feature running. The software has been divided in two sorts of modules, a communication module and a feature module. The communication modules are for example the database module and the CORBA module. Both these modules are a part of the information transportation system that all the communication modules handle.

Each module handles a special medium like database connection. The cause of this design choice is based on flexibility as Saab needs to provide all its products with flexibility due to a very demanding customer selection. This solution makes it possible to exchange communication modules in an easy way to change the product in almost unlimited ways. For example, if there is no possibility to get a network access, the communication module that handles the database connection is useless, so then it could be useful to exchange this module for another module that instead saves information to a hard drive or memory card.

This possibility to exchange communication modules will increase the lifetime of the system due to the ability to change parts as the backend systems and customer demands change. Also this type of design would be easier to maintain and upgrade to updated hardware, as only the incompatible parts have to be adjusted instead of the whole solution.

The feature modules represent code that implements different functions in the system, for example the error code handler and the temperature monitoring. The demand for different features could be very different from case to case, as the customers are using the equipment in several different environments together with equipment from other suppliers. The idea with feature modules is that there could be a range of available features that could be selected to each customer application. Also the possibility to add new features easily will create an opportunity to be able to customize the customer solution more, thereby increasing the customer value of the product.

5.5 Case study

A study has been made to gather information about what information that could be useful both for the end customers and for the engineers at Saab. This study is based on an online survey that has been sent out to a group of chosen engineers at Saab. In the survey there was a question about what their fields of expertise were, for example hardware, software, or verification. After that there was an open area for writing ideas and information that they wanted to use the system for. The general opinion is that there is a big security matter to be able to use any equipment of this type, due to that many customers don´t trust anyone and will not risk having a data connection to a business in another country.

A discussion with some of the Saab employees, who had read the results of the surveys, lead to the opinion that it would be good if there were two sides of the system. One side could be a system that the customer could use for controlling their fleet of vehicles, a so called customer management system. The twist here is that only the customer has access to the system. The information will be uploaded to the customer´s system and there will be no involvement of any stakeholder. In this type of setup there could be many advantages for customers due to that it is easier to get good knowledge of the health of the fleet and thereby do better strategic moves.

The other side of the system is an engineering based approach. The engineers at Saab can use the system in test and verification purpose. During development Saab has a number of GAMBs in their workshops. Often when they install software they start the installation and go away while it proceeds. The installation can take a while and if the installation encounters an error during that time, the engineer may not notice until several hours later. The STU can help prevent the loss of those hours by immediately noticing the engineer that something has gone wrong, thus saving time and money.

There are occasions when faults only show up at random times. It is time consuming to have an engineer waiting for that to happen or even impossible if the faults only happen when the equipment is in use at the customer. If the customer could connect the STU when a radar station is malfunctioning, an engineer wouldn’t have to travel to that place. This would be easy for the customer and would save money for Saab.

5.5.1 Saab security criteria

The responsible for IT security staff of Saab presented the following main security requirements that have to be followed at Saab

1. *Traceability*

There should be records of whoever has done what and at what time. If someone has tampered or done anything suspicious within the system, it should be possible to find out exactly who did it.

2. *Information security*

There should be sufficiently advanced cryptography and authentication processes to secure the classified information. If the sensitivity of the information is low, there may not be any need of cryptography. The inverse could mean that very advanced algorithms are necessary to guarantee that no information is leaked.

3. *Disaster recovery*

If the security is somehow compromised, there should be a direct disaster recovery plan to follow. To be able to have the telematics solution in Sweden, a number of instances have to approve of it. Among them are MUST and FMV. On the other hand, if it is supposed to be used by a customer in another country, it is entirely up to that country to approve of it. Therefore it may be the case that it is easier to focus the product to be something that the customer uses, rather than something that Saab uses internally.

5.6 Security measures

A special communication model has been developed to reduce the security gap that the system creates by connecting the equipment to a wireless network. This connection creates a possible opening for intrusion. In order to prevent any intruder from compromising the STU, a communication model were no data is sent directly to the connected diagnostic unit is used. There are no incoming connection possibilities from the wireless network into the unit. The communication is instead done only by the connected unit. The linked unit fetches data from a database server and sends information back to the same (or another) database server. A secured fileserver is used for more data consuming information. The important difference is that no communication is done directly towards the unit, and therefore it is impossible to exploit any other functions than those that are supported by the software.

Even if there is an intrusion into the database servers, the supported communication is controlled by the unit that has no direct access from the database servers. To secure the information that is sent to the database server, a crypto cipher is used to encrypt all data that have to be secured. The information that is sent to the database server is encrypted already before it is sent out to the server, just to secure that no data can be stolen on the way to the database server. The standard procedure for database crypto is that the database server encrypts the information. The problem with this is that the information then is insecure a long way over the communication channel. A standard encryption method named AES-128, see section 2.11Advanced Encryption Standard (AES), is used to secure the information on the way to the database server and also when it is stored in the database. The communication that consumes larger data transfers is using the SSH file transfer protocol, SFTP. This protocol supports various advanced crypto ciphers to create a secure line to the destination server.

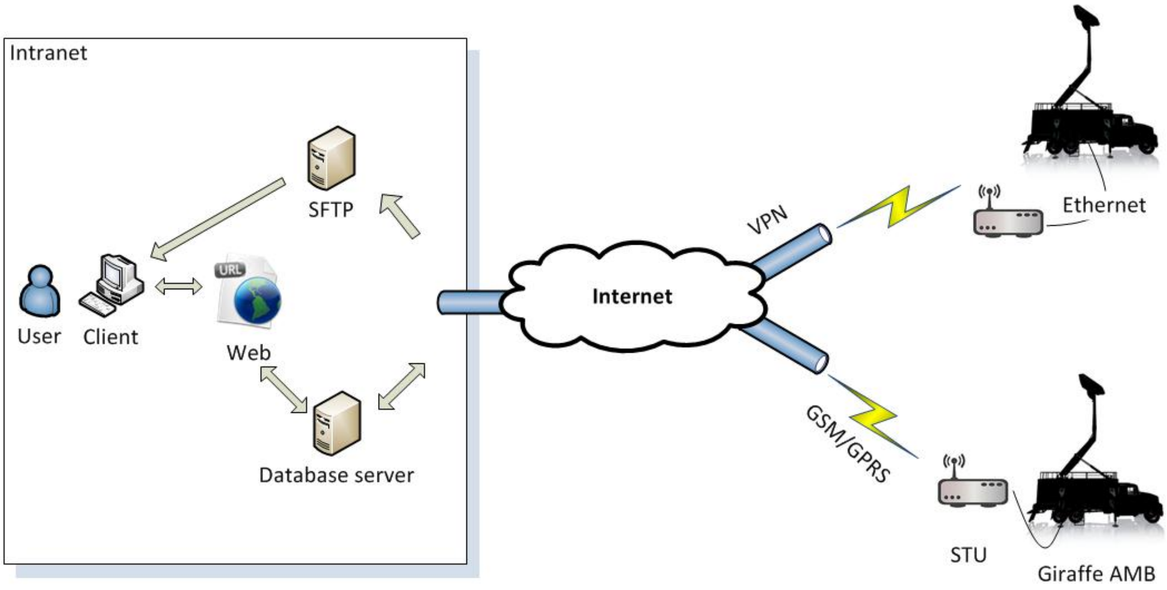


Figure 4. System overview

5.7 Identified benefits for Saab's customers

By adding a telematics function to a product, possibilities for new functions appear. Many of these functions that could be added could add more customer value into many products. Especially if the product is a field unit that moves around and just is a part of a bigger group of products like in our case, mobile radar stations. Based on the case study, some benefits and usage areas for the customer have been identified.

Military personnel would have great help in the planning of strategic moves if they had a top down view of their units in the field. The basic functionality of this top down view would be to show whether or not all units are working correctly. When planning military strategies, there is no need to know the exact problem with a faulty unit, it is enough to know if the unit is operational or not. This could be done by displaying all radar stations on a map with the faulty ones highlighted in red, figure 5.

As the strategic command could use a more basic interface with operational information, the maintenance team could use a much more detailed view that could show error codes and operational status from different nodes in the system. By getting a hint of the problem before getting the vehicle into repair or sending a repair team, time could be saved. Less time from fault to repair will automatically result in a more secure environment for both the repair team and the user of the equipment.

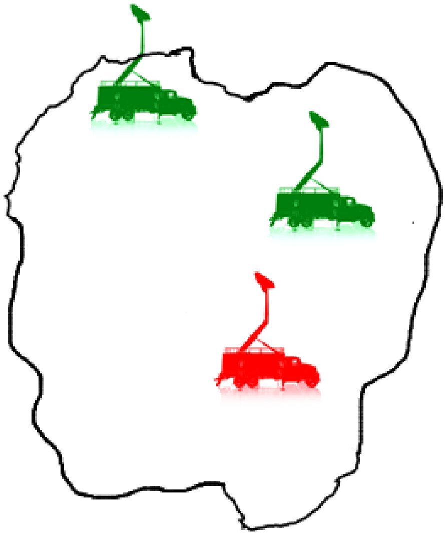


Figure 5. Operational and non-operational GAMBS in a map view

Engineers that want to diagnose the GAMBs remotely today must ask the customer to download files to a USB stick and then mail them to Saab. This tedious way is frustrating for the customer and takes unnecessarily long time. With the STU it is possible to immediately request and receive files from the GAMB.

6 Risk analysis

Entering the 21st century, information has been declared to be one of the most important building blocks in our daily life and social environment. As the importance of information has grown, the protection of valuable information has become increasingly important. To be able to protect information and defend against threats such as possible security breaches, it is important to be prepared. If a security breach would happen, a predetermined action plan should exist.

The goal with a risk analysis is to highlight the potential threats and what risks these threats can form. Based on the potential damage to the company, both financial and physical, an action plan based on the probability that the scenario could happen should be prepared.

The information that the radar station gathers is used to protect and maintain a social security. If the information in any way is unusable or wrong could have severe impact on the surroundings. In many cases a brake-down of the radar equipment could risk human life, which is impossible to set a financial value on. To calculate the risk of malfunctioning equipment due to a security breach in a tense defense situation is a challenge.

6.1 Potential threats and risks

A security evaluation has resulted in three possible types of attacks. The possible attack types are shown in figure 6 and further described in separate sections below.

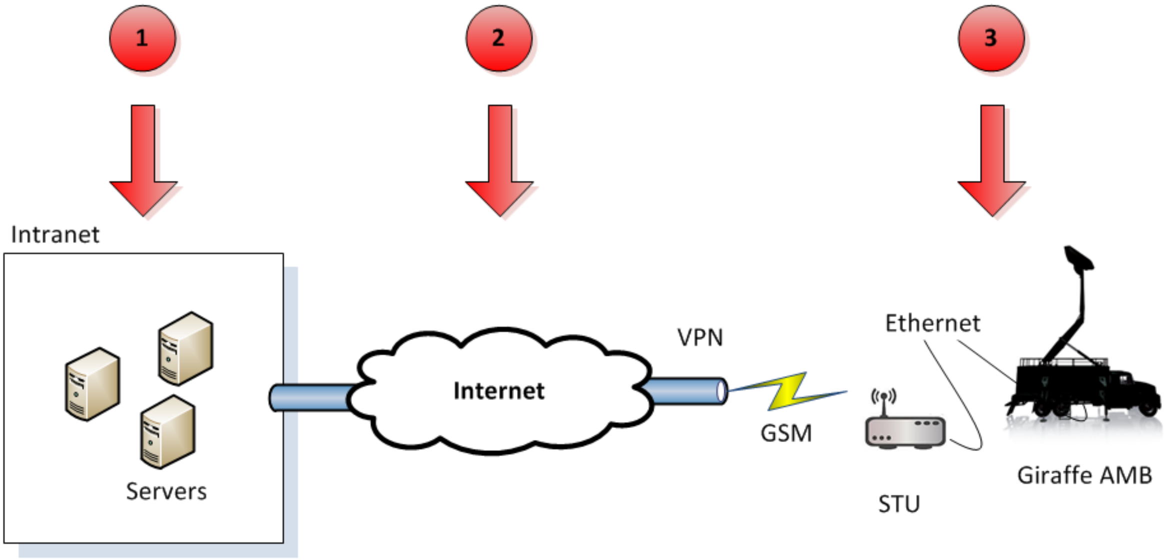


Figure 6. Potential places for attacks

6.1.1 Threat one – Server Attack

The diagnostic system is designed to use standard setups of server systems. The possibility to configure a server in several different ways creates a higher risk for security breaches. There are also cases where newly found security holes in server systems could be used to expose servers and their information.

The most secure alternative for a server environment would be to have separate servers for the diagnostics systems. Since the systems use standard servers, they will also have to use standard server protection, like firewalls and intrusion detection. The important part is that the servers should be separated from other local networks in order to limit the ways of connecting to the servers. If there is a workstation machine that has a physical connection to the servers, the workstation is often an easy target for intrusions just because the workstation has a major weakness, the human factor. The workstation can then act as a free ticket into the server environment.

Another important area of protection for servers, which in many cases is forgotten, is physical security. The physical placement of the server should protect from both intruders and faults created by human mistakes.

6.1.2 Threat two – Interception Attack

The diagnostic equipment will connect parts of the radar station to a public network, internet, which is a serious threat against the information and function that the radar station delivers. An ideal scenario for an enemy is to be able to make the equipment fail without entering their enemy's territory. But the probability that anyone without insider information would be capable of doing this is highly unlikely. That assumption is based on the case where the diagnostic equipment only is connected in conjunction with a service occasion. A service event could occur an unknown number of times per year, each time a failure is encountered. Assume that the equipment has two service occasions per year and that each service takes eight hours. During this time the equipment is connected to the internet for communication with a server. This connection to the internet is established using a GPRS connection without a static IP address. That means that a dynamic IP address is retrieved from the operator and that no one besides the provider knows what address has been assigned. To be able to start an attack against an internet-connected unit, the IP address has to be known, otherwise it would be impossible find the unit. Of course an enemy could take control over the GSM network and thereafter find out what the assigned IP address is and listen on all sent and received information, but that is unlikely.

Even if the enemy has the equipment and knowledge necessary to intercept the connection during this short window of time, the data is encrypted in two phases. The first phase is encryption of the information, with the encryption standard AES-128. The second phase is VPN tunneling of the data, which also uses a strong crypto standard.

Even though some sources state that AES-128 is an encryption that could be cracked, the time and resources for this would probably not be enough for the enemy to harm the radar station or be able to make use of any decrypted information.

Using a commercial system for communication could be an increased risk for the involved parties. If systems like GSM are used in a war situation, there is a risk that the actual position of the radar stations could be compromised. If the enemy has control over the wireless network, triangulation can be used to obtain the positions of radar stations that communicate with three or more GSM base stations. By using encryption on both voice conversations and data traffic over unprotected communication lines, that risk is minimized.

The worst problem with not having control over a communication channel, like GSM, is that the system could be made unavailable or disrupted by the enemy. Because of these risks, military versions of wireless networks have been developed. They can be locally deployed and used in this type of scenario. This type of system usually has a highly encrypted type of GSM connected to a locally deployed base station that communicates over a satellite connection.

6.1.3 Threat three – Physical Attack

A physical intrusion against the radar station is a scenario that always has been and always will be a major risk factor. There is a possible risk that encryption keys and similar could be retrieved if the enemy has physical contact with the system. But then it would be meaningless to get the encryption key to the wireless communication, as the secret information could be taken directly from the hard drives. To prevent the risk from someone who has gotten access to the encryption key, it can be exchanged before every service occasion.

6.2 Conclusion of risk analysis

If the enemy wants to make the radar station nonfunctional, electronic attacks will probably be very complex in comparison to alternatives like a physical attack. If an electronic attack would be used, the weakest point would probably be the server facility. If a physical security breach is the issue, the challenge would be to find out the location of the servers, as many companies have their server farms at secret locations. An attack from the internet against the servers would also be possible if any vulnerability in the servers' protection systems can be found or if the servers are badly configured.

The overall conclusion about the risks is that there are easier ways to take down a radar station than an electronic attack. If the goal is to gather secret information from the radar system, a major operation with money and resources has to be used to even get close to intercepting any information. Even if the enemies succeed in decoding encryptions and become able to intercept the diagnostic information, they are a long way from being able to get any other information from the radar station. This is due to that the communication model for the diagnostic systems is designed in such a way that they don´t receive any commands, they fetch the commands themselves. These commands will be executed on the radar's computers from an account with limited rights. The potentials for a successful electronic attack is very limited in all of the phases and will therefore probably also limit the interest of such attacks.

Warfare and defense in the 21st century is, as earlier described, a battle of information. Decisions in war that are based on both knowledge and information have better chances to succeed. Not to be forgotten is that an identified security breach can be turned against the enemy. Imagine if a security breach was identified and that the information that is transmitted could be exchanged to misleading information. That could create an advantage against the enemy.

There is one major risk with all military systems. If it in any context becomes known that an enemy or similar hostile individual has taken advantage of any part of the Saab system to get access to secret information. This would become more than a security leak. It would also become negative publicity for a company that specializes in security. There are significant amounts of money spent to maintain the value of the trademark, generated by their effective security solutions. These threats should therefore be valued as a risk for major financial losses.

7 Results

The proof of concept has shown that it is possible to create a telematics solution for Saab that maintains a high degree of security. Even though not all criteria have been met, for example traceability, those are not to challenging to implement. With the first prototype Saab Telematics Unit (STU), it is now possible to investigate how Saab can benefit from telematics. It is possible that other features may be more important than those that have been developed so far. For example, it could emerge that knowing the value of the charging power from the generators would be a great feature which hasn´t been implemented. The framework for getting this information is there and ready to be developed further with new features.

AES-128 is the encryption used by the STU. The motivation for this is that it wasn't possible to compile the encryption library Botan with the data type long long. The platform used lacked the support for long long, which was necessary for activating algorithms with keys of larger size, like AES-256. Whether this was due to software or hardware limits has not been determined yet. Even though another key size, like 256 bits, would have been desirable, AES-128 is still a good alternative. As is written in section 3.9 Advanced Encryption Standard (AES), NSA finds that AES-128 is sufficient to protect classified information up to the SECRET level. The only level above that is the TOP SECRET level, which would require AES-196 or AES-256. That should be an indication of how safe it is to use AES-128 in this system. The information can be compromised, but the risk is fairly small.

Much of the information that the STU retrieves from the radar station is collected with ordinary Linux commands via SSH. Since CORBA already exists in Saab's software platform, it would be good if all interesting information was available via that interface. That would make the STU completely platform independent and would also make the STU's software less complicated. It would require much work to move all information to CORBA, so this is not a realistic option. To move everything is not possible either, since it is very difficult to determine exactly what information would be needed in the future. But to minimize the need for customizing the STU when integrating it with new products, it would be good with as much information as possible available via CORBA.

Depending on the amount of data that needs to be monitored in the diagnostic system, the transfer speeds between the radar station and servers could be increased by upgrading to 3G or LTE for the wireless communication. The hardware would become marginally more expensive, but it should not be a deciding factor. The most important disadvantage with upgrading to a newer generation of mobile communications is that those systems use higher carrier frequency bands. That makes them less capable than GSM, which uses a low carrier frequency, to cover large areas.

The GSM communication should be considered as an example of a communication system that can be used for the diagnostic communication. There are many advantages with using a commercial system but there are also a couple of disadvantages which should be taken in mind before deciding upon such a system. The risk with using a commercial communication channel for the diagnostics could in some cases be worth the decreased security, compared to the alternative. The alternative to a telematics solution would be to send an engineer with the right skills to the radar station, which possibly is placed in a war zone. A fast diagnostic occasion to get the radar running could in some cases be worth a single hour of decreased security.

Power consumption is an important factor for systems that aren't connected to the power grid. The installation of a new unit will cause the power source to deplete quicker and thus reduce the power on time for the whole system. The power consumption of the STU, together with the estimated time that the whole system should be on, will decide if it is possible to power the STU from a battery or if it should be powered from the diesel generator, as the rest of the system.

Measurements of the power consumption for the STU and its separate parts are shown in the table below. All measurements were done at 12.5 V.

Table 1. Current and power for modem

Operation	Current [mA]	Power [mW]
Modem registering on network	80	1000
Idle	40	500

Table 2. Current and power for MX-4

Operation	Current [mA]	Power [mW]
Start up	170	2125
Idle	120	1500

Table 3. Operations of the full STU (both MX-4 and modem active)

Operation	Current [mA]	Power [mW]
Establishing GPRS connection	320	4000
Idle with GPRS established	200	2500
Main application running	250	3125

The results show that the STU does not require much power. An ordinary Li-ION battery with the correct voltage would deliver enough power to have it running for several hours. It would also be possible to power it from the diesel generators that the mobile radar stations have. In order to lower the power usage, the STU can be configured to update its values less often. That way the modem has to work less and power is saved.

The size of the database tables and how they increase over time affects how many radar stations that could be connected to the system before the servers run out of space. It is an interesting measure of how well the back-end part of the system scales.

The database consists of the nine tables shown in table 4. Besides storing information, the database is used to instruct the STU what to do. A user can create a custom command (standard Linux command) via the web portal. After that a row in the database will be added in the custom_command table, containing information about what the command was, and whether it has been executed or not. The STU sees that a custom command has been created and that it hasn't been performed yet and creates an errand. When the errand is done, a file with the results from the command is uploaded by the STU to a FTP server. The user can then access the file server and download the file. Another table that is used in a similar way is the log files table. As in the custom_command table is an errand created by the STU when it sees that a log file has been requested.

By transporting all information between the user and the STU via the database, an extra layer of security is introduced. Only validated data can be sent to the database and thus no invalid instructions can be sent to the STU.

Table 4. Database tables and their purposes

Name	Purpose
custom_command	Store all custom commands and whether they are complete or not
Errands	Track all errands and whether they are successful and complete
ErrorCodes	All errors collected from CEH
Harddrives	Amount of free space, etc.
logfiles	List of available log files
parameters	Different addresses and users for network connections, ie. SCP
signals	Signals read via CORBA from the DEM
Temperatures	All temperatures read from target
Users	Accounts information for the web platform

Other tables are continuously updated by the STU, instead of creating errands for a specific task. For instance, the temperatures table periodically receives new information from the STU about the system temperatures of the DEM computers and inserts that as new rows. This introduces the possibility to monitor the change of temperature in different nodes over time.

All data collected from the units is saved in a MySQL database. Depending on different design decisions that data will take different amount of space. One example of a database table is shown in table 5. The other database tables scale in a similar way.

Table 5. Structure of the temperature table

Column	Data type
TempId	Int(10) – 8 bytes
TempType	Varchar(20) – 20*1 byte
Temperature	Timestamp – 4 bytes
DeviceId	Int(10) – 8 bytes
Timestamp	Decimal(10,2) – 12 bytes

The total size of one row is 52 bytes. Given that one GAMB inserts the temperature every 10 seconds, it would take about 340 years to get 1 GB worth of temperature data. The calculation shows that there are no signs that the database will run into problems with disk space in the foreseeable future. Otherwise, it would have been necessary to do some database optimization. One easy fix would be to restrict the number of characters in strings, as an attempt to compress the tables.

There are many design choices along the path of development. For example instead of using MySQL, another database engine could have been used, for example Microsoft SQL or PostgreSQL. The reason for using MySQL was the readily available connectors for both C/C++, and C# and also previous experiences with that database engine. The way that the tables have been organized could most certainly have been designed in a smarter and more optimized way, but no further investigation has been done in that matter. It is quite possible that another database could fit this master thesis better. Even if that is the case, there is nothing that points to the fact that this database is not sufficient for this application. The size of the data that is stored in the database is relatively small and this lowers the demands for a highly optimized database.

The back-end system has been developed so that no special server hardware or software is necessary. Standard web servers together with standard database servers are the core of this back-end solution. The main goal with this approach is that the system should be easy and cheap to implement into existing infrastructure. Standard equipment usually works together without problems. It also makes the solution very scalable due to the fact that standard servers today are both inexpensive and easy to acquire. The everyday user will only come in contact with this system from the web platform and therefore it is very important that this web interface is practical and easy to understand. As the case study has pointed out, we have two possible tracks for customizing the user experience of the system. The two tracks are:

- Engineering tool
- Customer management system

The benefit of the STU as an engineering tool is that it is possible for an engineer to observe the status and compare many different radar stations at the same time. If the engineers install an update, they can immediately detect if something goes wrong and quickly fix it. This can potentially save both time and money. The ability to monitor different values over time can help the engineers to find and eliminate intermittent bugs. Those are bugs that happen from time to time but are hard to reproduce. In order to eliminate the bugs, a large amount of data can help to find the root-cause and thus give a hint of how to fix them.

When the STU is used as a customer management system, it is possible for the customer to observe the health of their radar stations in almost real-time. In a war situation it can be a great advantage to immediately see if something has happened with the radar.

One of the good things with the STU is that it is both easy to integrate with Saab's products as well as leave it out. It can be up to the customers to decide if they want to procure this feature. They can also choose when it should be active, if the program should be integrated with Saab's computers or if it should be a completely stand-alone solution. For some customers, it may only be interesting to use the STU during service errands. In that case, they can plug it in for a short period of time and let the engineers at Saab read whatever data they want from the radar station. The many possibilities make the STU very versatile.

8 Conclusion

The Saab Telematics Unit (STU) communicates with the database, Saab computers and file servers and can apply encryption where needed. A number of different algorithms for encryption are available, currently is AES-128 used. GSM and 3G are available for wireless connection between the STU and the servers. VPN tunneling is supported by the STU and can be enabled to further increase the security.

It is still a way to go before establishing telematics at Saab. The technical solution must have taken sufficient security measures in terms of encryption, authentication and traceability. After convincing the decision-makers at Saab that the STU reaches the necessary security levels, the external players must also be convinced. Försvarets materielverk (FMV) and Militäraunderrättelsetjänsten (MUST) have to approve before it can be used in Sweden.

For some of the most demanding customers, more security measures can be taken. The easiest solution is to minimize the amount of critical information transferred in the system. Other solutions are to increase the level of encryption, use more secure authentication processes and to use a dedicated hardware to setup the VPN tunnel between the STU and the back-end.

Another factor that must be considered is that even information that is not secret can become a risk together with other non-secret information. An example of this could be the information that the radar vehicle has 200 liters of fuel and the support legs is in unlocked position. This information could be considered non-secret information, but together they describe how long time it would take to deploy the equipment in another position with the range of 200 liters of fuel.

To be able to minimize the possible damage from an enemy who has gotten hold of secret information, a study of the impact of possible security breaches should be done. This study should also cover counter tactics if that would happen. If there is a fixed procedure for situations where a possible security breach has been encountered, that would validate the use of the system even if there is a small possible risk that information could leak.

The system is running on a standard Linux platform and the applications could be moved to Saab's own computers and thus could all external hardware, except the GSM/GPRS modem, be removed. The cost of such a system would be very low.

A user friendly web platform must be developed. It would be preferable if it had different modes depending on the user. Technicians generally require more technical and specific data compared to regular military personnel. A thorough study of the different stakeholders need is necessary to design the web platform in such a way that every user can make the most of it.

Even more features can be implemented to increase the usefulness of the system. These are some of examples of features that could be added:

- GPS
- Accelerometer
- CAN
- Interface
- Temperature sensors

A CAN-bus interface can be used to get vehicle information. One feature that has been requested is to be able to get information about the current fuel level in the diesel generators. An accelerometer can be used to get information about the vehicles operation. Has it been exposed to extreme accelerations in a certain direction? That may be an indication of reason for failure. Such acceleration would happen if, for example, the vehicle has rolled on the side because of incorrect use of the support legs. This kind of information could be important in warranty issues. Temperature sensors could also be used as a tool in troubleshooting the product. Has it been exposed to extreme temperatures before failure?

There are some different paths of direction that the STU could take. It could strictly be used as a diagnostics tool that is active only when manually connected to the radar station. Another option is to always have it connected but only activate it when wanted. Or it could be something that is always connected and active. There are trade-offs with each solution. When the STU is only connected for a short period of time, the security is of lesser concern, but the product's main purpose is reduced to ease of data retrieval. If it is connected and active all of the time, the security becomes more of a concern. The main advantage is that it is easier to collect information over a long time, which could lead to improved serviceability.

One feature that is desired is software download. To be able to patch a system remotely and add features would reduce a considerable amount of maintenance cost. Instead of having an engineer travel to the customer, most often abroad, in order to update the software, it would be possible to just download and install new software via the STU. For this to be feasible would require extremely rigorous security measures. Software download is probably not achievable considering the implications of a security breach.

This realization and deployment of telematics together with the military equipment from Saab has been successful. The development of the prototype STU has verified that it is possible to develop this proof of concept to a real product. The biggest obstacle is to convince engineers and customers. There is still a fear, among some of them, of sending secret information through a medium that is not of military control. With the help of advanced cryptographic algorithms, even wireless data can be secured.

Bibliography

Addison, D. (2001). Embedded Linux applications: From wrist watches to cluster-based supercomputers. *DeveloperWorks* .

Advanced Encryption Standard. (2012, May 22). Retrieved May 24, 2012, from Website: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Block cipher modes of operation. (2012, May 23). Retrieved May 24, 2012, from Wikipedia: http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

Bogdanov, A., Khoratovich, D., & Rechberger, C. (2011). *Biclique Cryptanalysis of the Full AES.* K.U. Leuven, Belgium; Microsoft Research Redmond, USA; ENS Paris and Chaire France Telecom, France.

Chen, W. Y. (2001, 01 01). *AccessScience.* Retrieved 04 01, 2012, from Asymmetrical digital subscriber line (ADSL): http://www.accessscience.com.proxy.lib.chalmers.se

CNSS. (2003). *CNSS Policy No. 15, Fact Sheet No. 1 National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security.* Ft Meade MD.

Freescale Semiconductor. (2012, 01 01). Retrieved 04 02, 2012, from Product Longevity: http://www.freescale.com/webapp/sps/site/overview.jsp?code=PRDCT_LONGEVITY_HM

General Packet Radio Service. (2012, March 20). Retrieved May 24, 2012, from Wikipedia: http://sv.wikipedia.org/wiki/General_Packet_Radio_Service

Gottesdiener, E. (1995). RAD Realities: Beyond the Hype to How RAD Really Works. *Application Development Trends* .

Grisby, D. (2008, February 14). *The OMNI Naming Service*. Retrieved May 29, 2012, from omniORB: http://omniorb.sourceforge.net/omni41/omniNames.pdf

Host Mobility. (2012, 01 01). Retrieved 04 01, 2012, from Host Mobility MX-4 Fordonsdator: http://www.hostmobility.net/documents/Produktblad_MX-4A.pdf

Kirch, O., & Dawson, T. (2000). The Point-to-Point Protocol. In *Linux Network Administrator's Guide* (2nd Edition ed.). O'Reilly.

Lewandowski, S. M. (2008). *Client-server system*. Retrieved May 24, 2012, from AccessScience: http://www.accessscience.com

Machine-to-machine. (2012, April 26). Retrieved May 24, 2012, from Wikipedia: http://en.wikipedia.org/wiki/Machine-to-Machine

Mackerras, P. (2012). *PPPD manual page*. Retrieved May 24, 2012, from ppp web pages: http://ppp.samba.org/pppd.html

McHale, C. (2007). *CORBA EXPLAINED SIMPLY*. Retrieved 4 1, 2012, from http://www.ciaranmchale.com/corba-explained-simply/

Misa, T. (2004). Telegraphs and public works. In *Leonardo to the Internet: Technology and Culture from the Renaissance to the Present* (pp. 104-112).

MySQL. (2012, May 13). Retrieved May 24, 2012, from Wikipedia: http://en.wikipedia.org/wiki/Mysql

OMG. (2012, 08 03). *About OMG*. Retrieved 04 1, 2012, from http://www.omg.org/gettingstarted/gettingstartedindex.htm

OMG. (2004, 09 01). *OMG.* Retrieved 04 01, 2012, from Naming Service Specification: http://www.omg.org/spec/NAM/1.3/PDF/

OmniORB. (2008, 02 14). Retrieved 04 01, 2012, from The OMNI Naming Service: http://omniorb.sourceforge.net/omni41/omniNames.pdf

Pechanec, J. (2007, July 9). *How the SCP protocol works* . Retrieved May 24, 2012, from Oracle Blogs: https://blogs.oracle.com/janp/entry/how_the_scp_protocol_works

Salman, T. E. (2011). *Diagnosis in Automotive Systems: A Survey.* Pittsburgh: Carnegie Mellon University.

Satellite Internet access. (2012, May 17). Retrieved May 24, 2012, from Wikipedia: http://en.wikipedia.org/wiki/Satellite_Internet_access

Secure copy. (2012, February 28). Retrieved May 24, 2012, from Wikipedia: http://en.wikipedia.org/wiki/Secure_copy

Secure Shell. (2012, May 14). Retrieved May 24, 2012, from Wikipedia: http://en.wikipedia.org/wiki/Secure_Shell

SSH File Transfer Protocol. (2012, May 19). Retrieved May 24, 2012, from Wikipedia: http://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol

Tode, G. (1998). Tekniken utvecklas - människan förblir densamma. *FOA-tidningen* .

Valenzuela, R. A. (2007). *Mobile communications*. Retrieved May 24, 2012, from AccessScience: http://www.accessscience.com

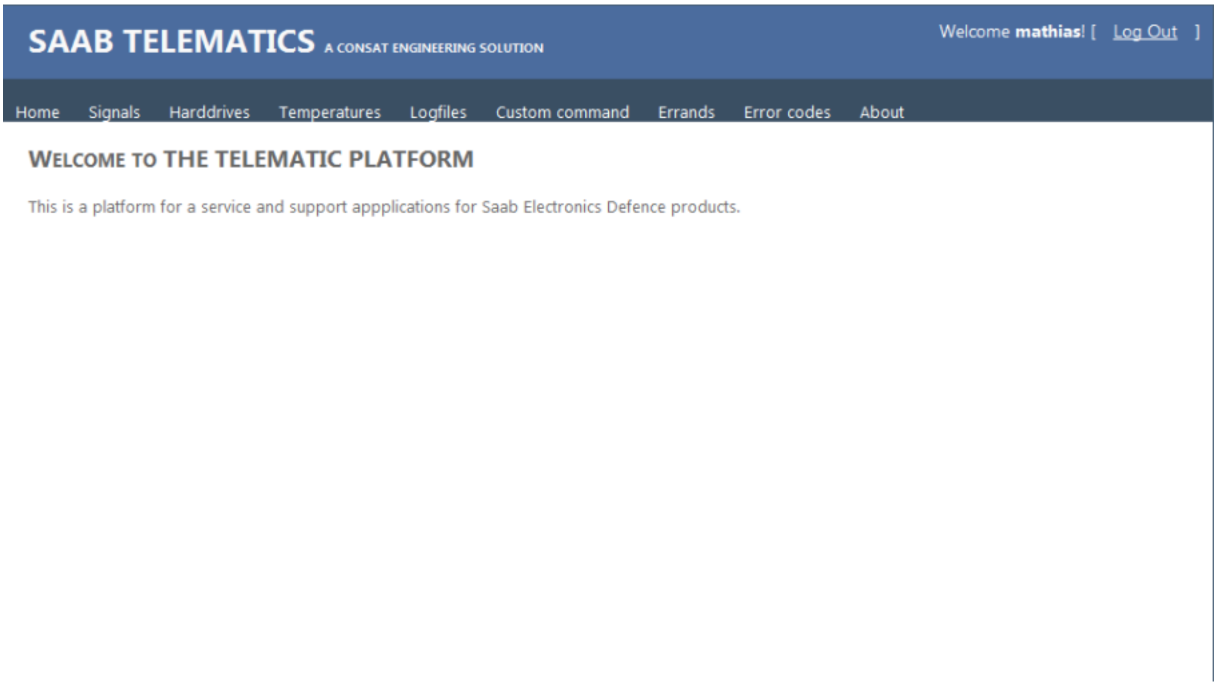
WirelessCar. (2012, 01 01). Retrieved 04 01, 2012, from Volvo On Call, Volvo Cars: http://www.wirelesscar.com/?page_id=26

Xunhua, W., Coppersmith, D., Matyas, S. M., & Meyer, C. H. (2008). *Cryptography*. Retrieved May 24, 2012, from AccessScience: http://www.accessscience.com

Ylonen, T. (1996). SSH - Secure login connections over the internet. *Proceedings of the 6th conference on USENIX Security Symposium, Focusing on Applications of Cryptography - Volume 6* (pp. 4-4). USENIX Association Berkeley, CA, USA.

Appendix A

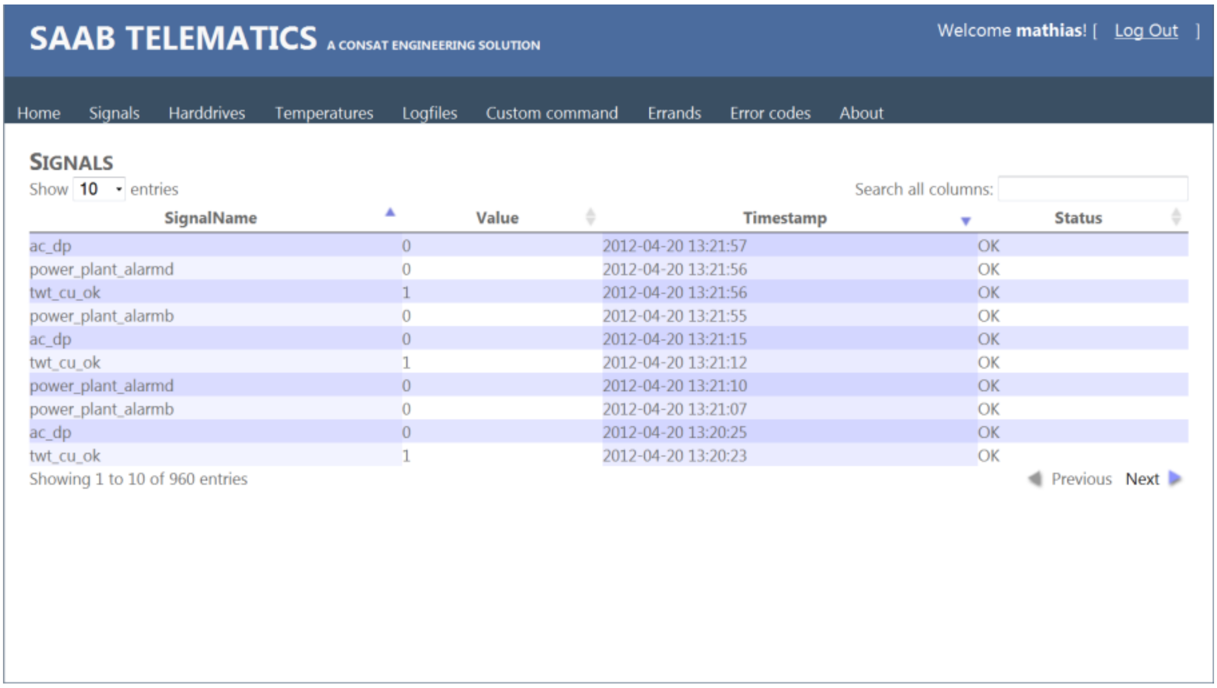
The web platform is presented in this appendix as a series of figures.



WELCOME TO THE TELEMATIC PLATFORM

This is a platform for a service and support appplications for Saab Electronics Defence products.

Figure 7. Home



SIGNALS

Show 10 entries

Search all columns:

SignalName	Value	Timestamp	Status
ac_dp	0	2012-04-20 13:21:57	OK
power_plant_alarmd	0	2012-04-20 13:21:56	OK
twt_cu_ok	1	2012-04-20 13:21:56	OK
power_plant_alarmb	0	2012-04-20 13:21:55	OK
ac_dp	0	2012-04-20 13:21:15	OK
twt_cu_ok	1	2012-04-20 13:21:12	OK
power_plant_alarmd	0	2012-04-20 13:21:10	OK
power_plant_alarmb	0	2012-04-20 13:21:07	OK
ac_dp	0	2012-04-20 13:20:25	OK
twt_cu_ok	1	2012-04-20 13:20:23	OK

Showing 1 to 10 of 960 entries

Figure 8. Signals

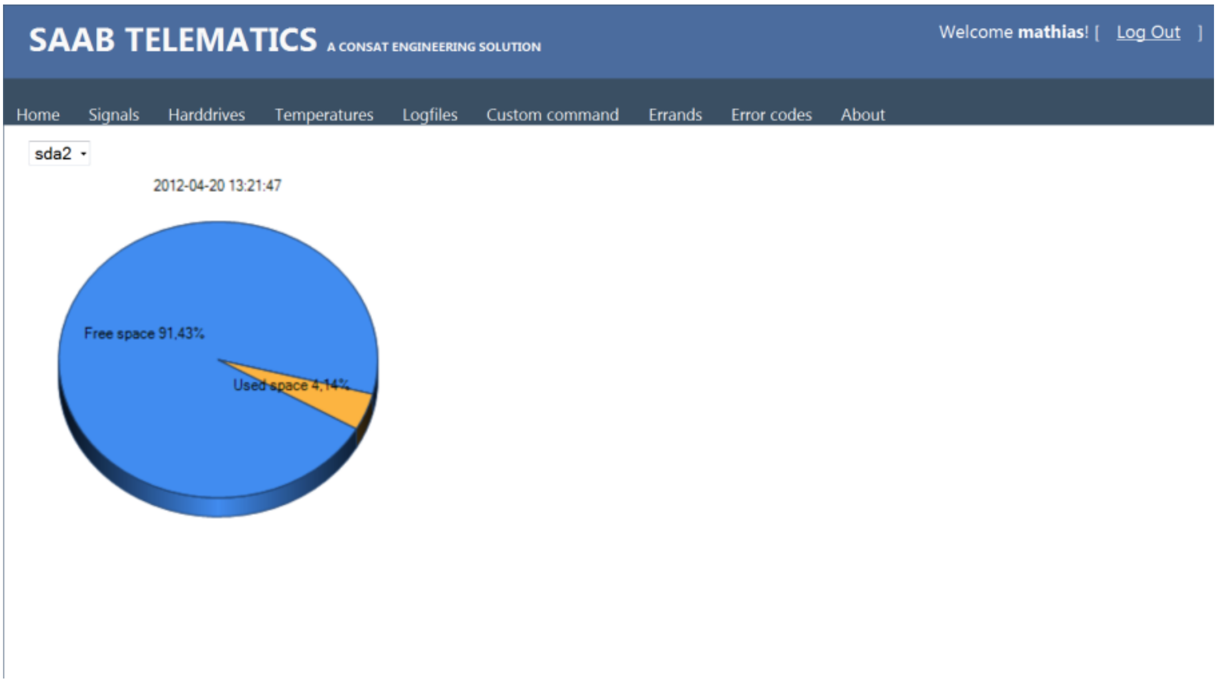
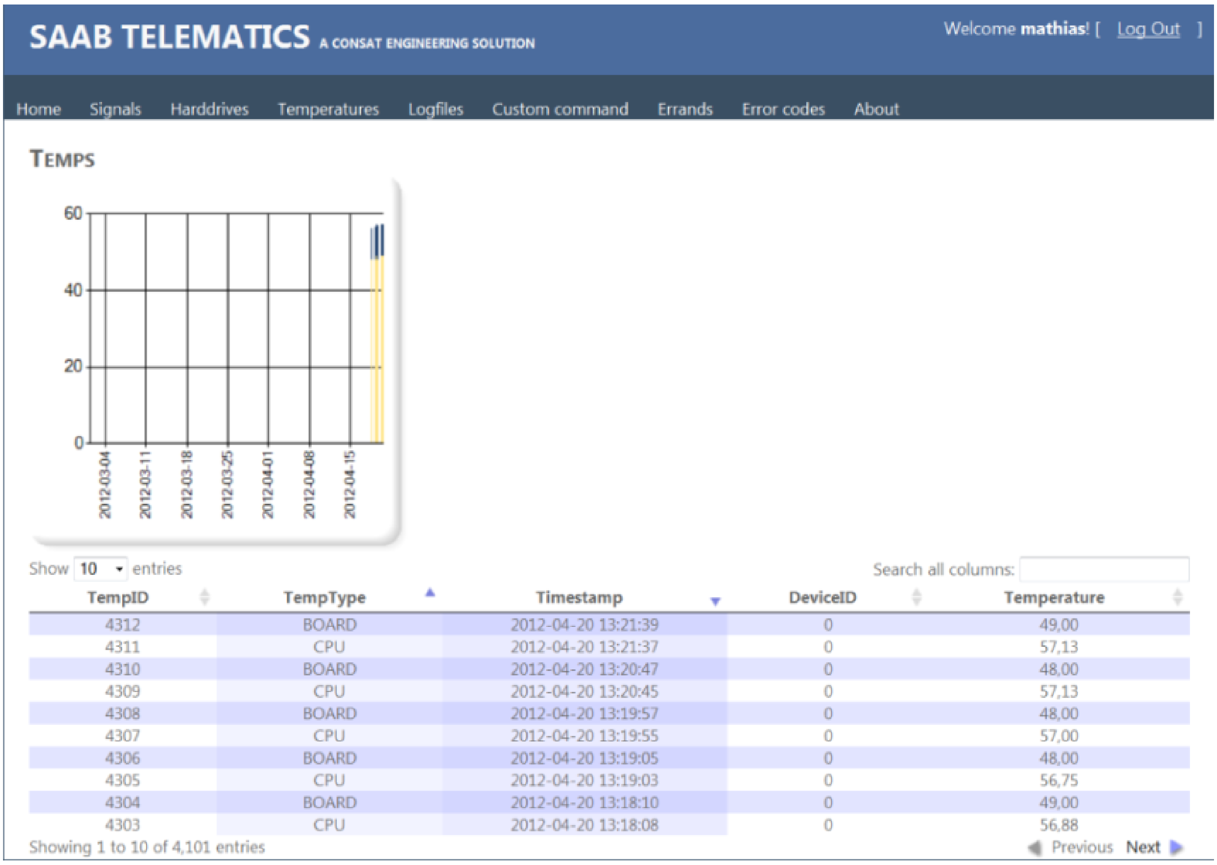


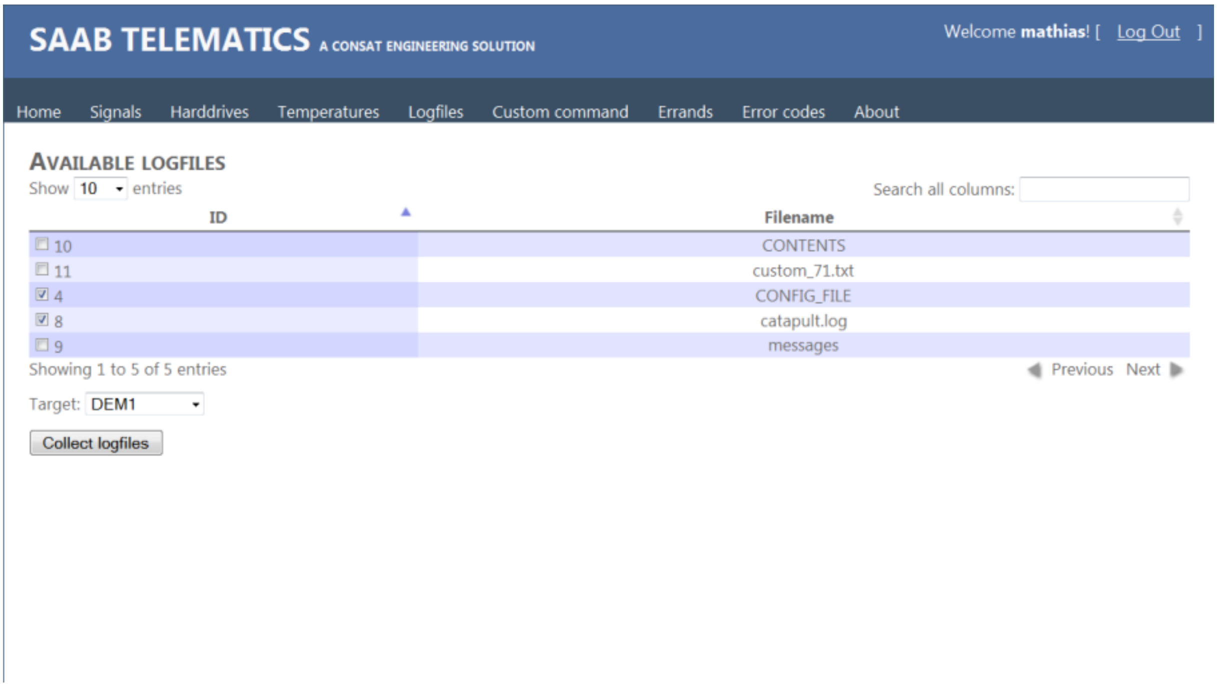
Figure 9. Harddrives



TempID	TempType	Timestamp	DeviceID	Temperature
4312	BOARD	2012-04-20 13:21:39	0	49,00
4311	CPU	2012-04-20 13:21:37	0	57,13
4310	BOARD	2012-04-20 13:20:47	0	48,00
4309	CPU	2012-04-20 13:20:45	0	57,13
4308	BOARD	2012-04-20 13:19:57	0	48,00
4307	CPU	2012-04-20 13:19:55	0	57,00
4306	BOARD	2012-04-20 13:19:05	0	48,00
4305	CPU	2012-04-20 13:19:03	0	56,75
4304	BOARD	2012-04-20 13:18:10	0	49,00
4303	CPU	2012-04-20 13:18:08	0	56,88

Showing 1 to 10 of 4,101 entries

Figure 10. Temperatures



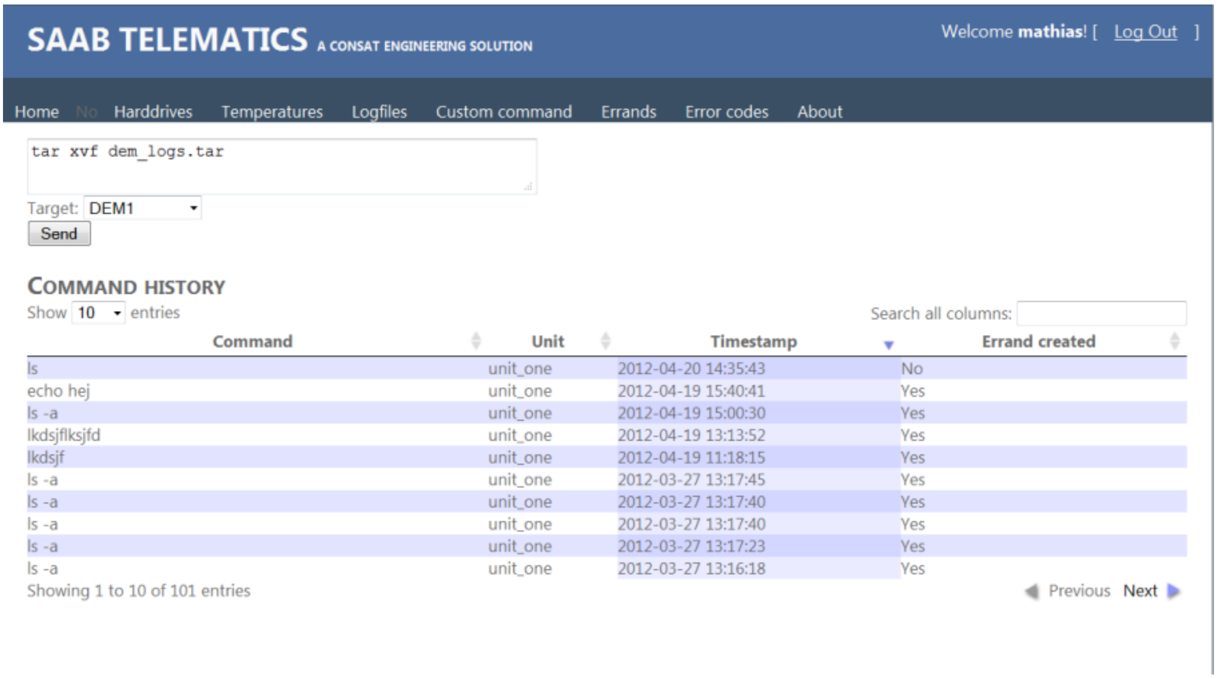
Available logfiles

ID	Filename
☐ 10	CONTENTS
☐ 11	custom_71.txt
☑ 4	CONFIG_FILE
☑ 8	catapult.log
☐ 9	messages

Showing 1 to 5 of 5 entries

Target: DEM1

Figure 11. Log files



```
tar xvf dem_logs.tar
```

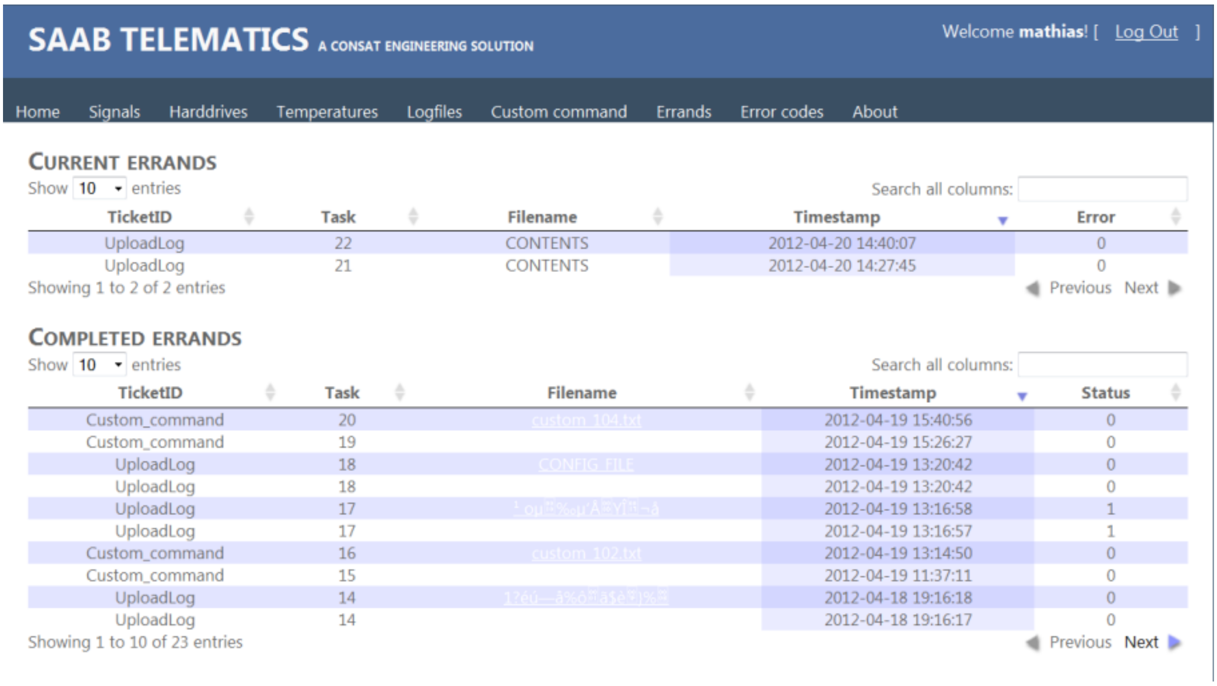
Target: DEM1

Command history

Command	Unit	Timestamp	Errand created
ls	unit_one	2012-04-20 14:35:43	No
echo hej	unit_one	2012-04-19 15:40:41	Yes
ls -a	unit_one	2012-04-19 15:00:30	Yes
lkdsjflksjfd	unit_one	2012-04-19 13:13:52	Yes
lkdsjf	unit_one	2012-04-19 11:18:15	Yes
ls -a	unit_one	2012-03-27 13:17:45	Yes
ls -a	unit_one	2012-03-27 13:17:40	Yes
ls -a	unit_one	2012-03-27 13:17:40	Yes
ls -a	unit_one	2012-03-27 13:17:23	Yes
ls -a	unit_one	2012-03-27 13:16:18	Yes

Showing 1 to 10 of 101 entries

Figure 12. Custom command



CURRENT ERRANDS

TicketID	Task	Filename	Timestamp	Error
UploadLog	22	CONTENTS	2012-04-20 14:40:07	0
UploadLog	21	CONTENTS	2012-04-20 14:27:45	0

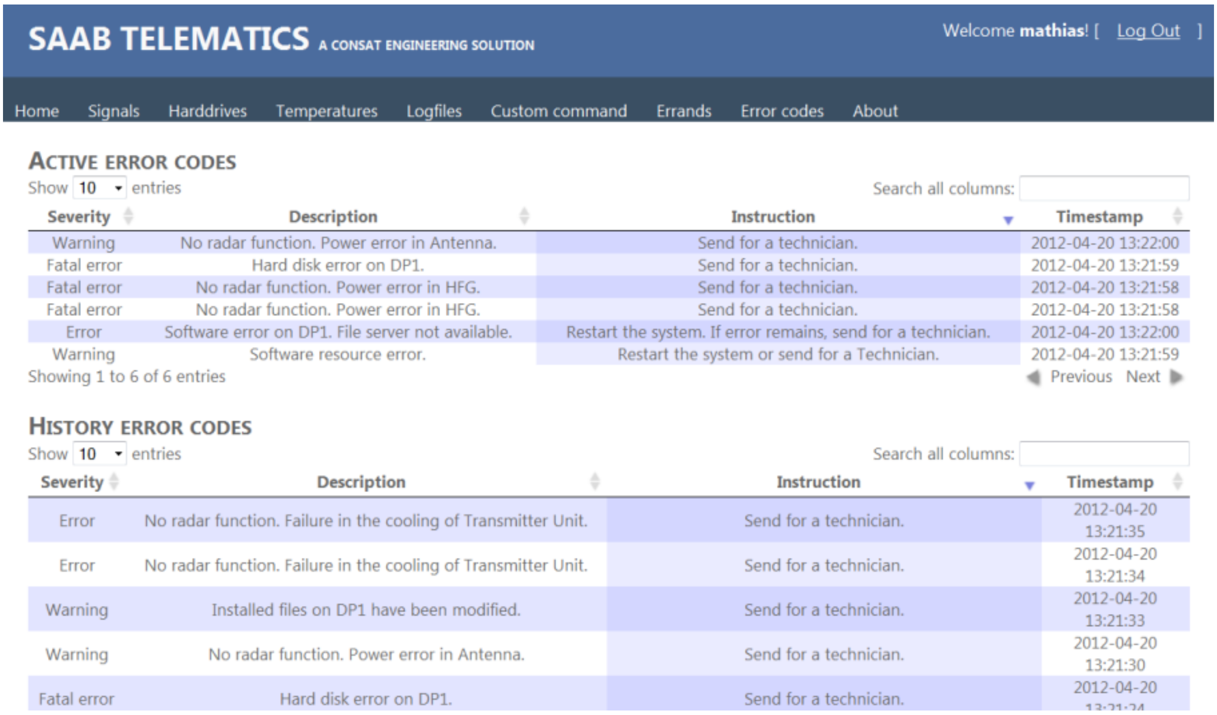
Showing 1 to 2 of 2 entries

COMPLETED ERRANDS

TicketID	Task	Filename	Timestamp	Status
Custom_command	20	custom_104.txt	2012-04-19 15:40:56	0
Custom_command	19		2012-04-19 15:26:27	0
UploadLog	18	CONFIG_FILE	2012-04-19 13:20:42	0
UploadLog	18		2012-04-19 13:20:42	0
UploadLog	17	[illegible]	2012-04-19 13:16:58	1
UploadLog	17		2012-04-19 13:16:57	1
Custom_command	16	custom_102.txt	2012-04-19 13:14:50	0
Custom_command	15		2012-04-19 11:37:11	0
UploadLog	14	[illegible]	2012-04-18 19:16:18	0
UploadLog	14		2012-04-18 19:16:17	0

Showing 1 to 10 of 23 entries

Figure 13. Errands



ACTIVE ERROR CODES

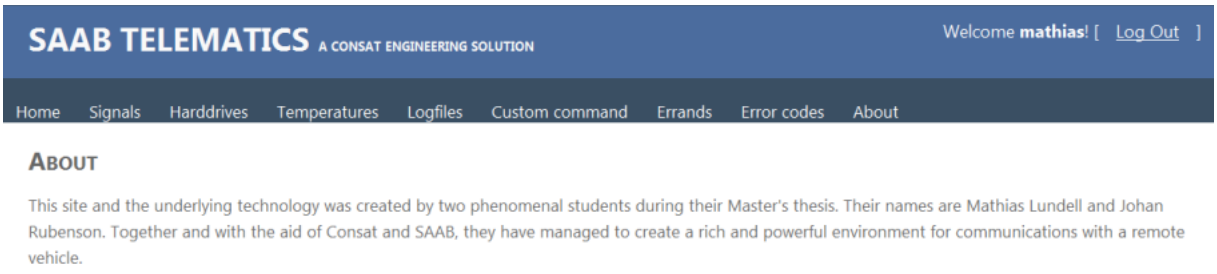
Severity	Description	Instruction	Timestamp
Warning	No radar function. Power error in Antenna.	Send for a technician.	2012-04-20 13:22:00
Fatal error	Hard disk error on DP1.	Send for a technician.	2012-04-20 13:21:59
Fatal error	No radar function. Power error in HFG.	Send for a technician.	2012-04-20 13:21:58
Fatal error	No radar function. Power error in HFG.	Send for a technician.	2012-04-20 13:21:58
Error	Software error on DP1. File server not available.	Restart the system. If error remains, send for a technician.	2012-04-20 13:22:00
Warning	Software resource error.	Restart the system or send for a Technician.	2012-04-20 13:21:59

Showing 1 to 6 of 6 entries

HISTORY ERROR CODES

Severity	Description	Instruction	Timestamp
Error	No radar function. Failure in the cooling of Transmitter Unit.	Send for a technician.	2012-04-20 13:21:35
Error	No radar function. Failure in the cooling of Transmitter Unit.	Send for a technician.	2012-04-20 13:21:34
Warning	Installed files on DP1 have been modified.	Send for a technician.	2012-04-20 13:21:33
Warning	No radar function. Power error in Antenna.	Send for a technician.	2012-04-20 13:21:30
Fatal error	Hard disk error on DP1.	Send for a technician.	2012-04-20

Figure 14. Error codes



ABOUT

This site and the underlying technology was created by two phenomenal students during their Master's thesis. Their names are Mathias Lundell and Johan Rubenson. Together and with the aid of Consat and SAAB, they have managed to create a rich and powerful environment for communications with a remote vehicle.

Figure 15. About

Appendix B

The following page will present the digital survey that has been used to get input in the development phase based on the Rapid Application Development method. It also include a summary of the answers of the survey.

CHALMERS CONSAT SAAB

Hi

We are doing a master thesis for developing a telematic system for SAAB. This telematic system will create a possibility to get status reports from a vehicle, ie SAAB Giraffe, to determine faults and possible service adjustments.

There has been a lot of discussions about what information in the system that is relevant to transmit. So we have decided to create a few user cases. By filling in this form, you can transfer the knowledge of what information that could be useful to us.

The system will be connected to the main frame computers by ethernet and it will be possible to communicate with the other computer-modules in the framework. Both corba and other communication protocols will be available. This information will then be sent by GPRS or similar a technologies to a database server for further processing.

Name*

E-Mail*

What type of projects do you often work with*

○ Software
○ Hardware
○ Verification
○ Production
○ Other

What type of data can be useful for your projects? (example temp, voltage, signal)

If we want to discuss your ideas, could you give us a date there you can spend a few minutes of your time?

Contact information:

Chalmers:
Johan Rubenson, 0709-998725, rubenson.johan@gmail.com
Mathias Lundell, 0703-073262 , lundell.mathias@gmail.com
Consat: **Stefan Engström**
Saab: Anders Martinsson

Submit Page 1 of 1

Powered by Adobe FormsCentral | Terms of Use | Report Abuse

Survey answer 1

Behovet gäller nog det mesta, så som spänning, temperatur, luftfuktighet, flöde (vatten), start tillfällen m.fl. Givetvis så är det även stort intresse av hantering (bra hantering) av loggad data i systemet också. Vi har/kommer ha av att monitorera nyttjande av system då vi inte är på plats detta eftersom kunden i vissa fall får köra våra system utan våran närvaro. Info om nyttjande profil mm. är viktig att ha då man t.ex. hamnar i diskussioner om ersättning vid eventuellt felutfall och reparation av produkten.

- Spänningar
- Luftfuktighet
- Vatten flöde
- Starttillfällen
- Loggdata hantering
- Loggning av system utnyttjande? Nyttjande profil?

Survey answer 2

ofiltrerad fellista systemloggar, men i nuvarande tappning ligger den fil man får i format xxx.tar.7z eftersom den kan bli rätt stor. Så får man ut filen skall det gå att packa upp, enkelt skicka info till ngn samt lägga över info på en server. dessutom kunna skicka in "stop" signal vid uppstart samt skriva linux kommandon. så det är en del som skall klaras av för att konkurrera ut en PC som vi alltid har med i alla fall. Har man dessutom en pc med väldigt snabb uppstart så blir det jobbig konkurrens.

Survey answer 3

Temperature, voltage, operational status, fluid levels, load etc. for the system and all its subsystems. Status information from all the systems computer nodes and network components. Datalogs, both from normal operation and system errors.

- Spänningar
- Temperaturer
- Status
- Vätske nivåer
- Belastning
- Loggdata

Survey answer 4

BIT-codes from the system incl. some system messages.

Survey answer 5

Felkoder, driftstider och driftsprofiler, radarstyrningar och inställningar.

Survey answer 6

De ingående delsystemen har oftast en inbyggd felhantering som rapporterar problem. Främst är det problemen vi är intresserade av. I vissa delsystem är felhanteringen bristfällig eller att den inte har byggts ihop med övriga systemet. Det är nog denna typ av data som jag personligen är mest intresserad utav (kan vara RF-signal, temp, volt, etc.)

Survey answer 6

Hi, Here comes a test of the questionnaire. Some of the intresting parameters could be; System uptime Temp both processor and environment in the cabin Hard drive status (freespace, badsectors, number of readings and writings?) Version of applicationsoftware and runtimeplatforms Processor load

- System uptime
- Temp cpu, enviroment
- Hard drive status (freespace, bad sectors, number of readings and writings)
- Application software
- Runtime plattforms
- Processor load