Improving Airplane Safety by Incorporating Diagnosis into Existing Safety Practice

Jonas Biteus, Gunnar Cedersund, Erik Frisk,
Mattias Krysander, and Lars Nielsen,

E-mail: {biteus, gunnar, frisk, matkr, lars}@isy.liu.se
Department of Electrical Engineering
Linköpings universitet, SE-581 83 Linköping, Sweden

Report: LiTH-ISY-R-2648
ISSN: 1400-3902

23th November 2004

Avdelning, Institution
Division, Department

Vehicular Systems,
Dept. of Electrical Engineering
581 83 Linköping

Datum
Date

23th November 2004

Språk
Language
☐ Svenska / Swedish
☒ Engelska / English
☐ _____

Rapporttyp
Report category
☐ Licentiatavhandling
☐ Examensarbete
☐ C-uppsats
☐ D-uppsats
☒ Övrig rapport
☐ _____

ISBN
—

ISRN
LITH-ISY-EX-LiTH-ISY-R-2648-2004

Serietitel och serienummer
Title of series, numbering

ISSN
1400-3902

URL för elektronisk version
`http://www.vehicular.isy.liu.se`

Titel Förbättring av flygsäkerhet genom att införa diagnos i existerande säkerhetsprocedurer

Title Improving Airplane Safety by Incorporating Diagnosis into Existing Safety Practice

Författare
Author Jonas Biteus, Gunnar Cedersund, Erik Frisk, Mattias Krysander, and Lars Nielsen

Sammanfattning
Abstract

Safety has always been at premium in airfare. There is a long history of systematic work in the field, and current practice has established a high degree of safety that has resulted in so low failure numbers that the public finds confidence in the process of air worthiness certification. However, the design and development process of airplanes to achieve this is costly and may be even more so since modern airplanes become more and more complex. Furthermore, recent trends towards *Unmanned Aerial Vehicles* (UAV) are likely to require even more efforts and costs, to fulfill the increased safety requirements. Therefore it is interesting to investigate modern techniques that promises to improve safety at reduced costs. One such technique is diagnosis. Diagnosis in general is a term that includes several research and application fields. Examples of such fields, that are technology drivers, are the fields of supervision both on-line (on-board) and off-line (on ground), operator support that evolved from the Harrisburg accident, and law based emission diagnostics regulation e.g. as stipulated by *California Air Resource Board* (CARB).

The current work is an investigation in the cross field between safety assessment and diagnosis techniques. The first step was to root the work in existing safety practice. This means that the Swedish defense procedure has been adopted as described in *H SystSäk E*. It is a safety framework that uses fault tree analysis and failure mode effect analysis as important tools. Thereafter some flight applications were investigated together with Saab specialists to capture and formulate some aspects that are non-trivial to cast in the existing safety framework. Examples of such aspects found are for instance related to performance requirements in different operational model. A principle case study was then formulated using laboratory equipment, with the aim to capture some of the identified aspects in the problem formulation. A complete process for safety analysis was then completed along the lines of *H SystSäk E* including all meetings and documents required therein. Several observations were done during this work, but the overall conclusion so far is that the effect of introducing diagnosis algorithms can be handled in the safety analysis, and, yes, that there is a promise that diagnosis algorithms can improve safety in a structured quantitative way by lowering the contribution to the total failure risk from the subsystem being diagnosed.

Nyckelord
Keywords diagnosis, safety, fta, fmea

Abstract

Safety has always been at premium in airfare. There is a long history of systematic work in the field, and current practice has established a high degree of safety that has resulted in so low failure numbers that the public finds confidence in the process of air worthiness certification. However, the design and development process of airplanes to achieve this is costly and may be even more so since modern airplanes become more and more complex. Furthermore, recent trends towards *Unmanned Aerial Vehicles* (UAV) are likely to require even more efforts and costs, to fulfill the increased safety requirements. Therefore it is interesting to investigate modern techniques that promises to improve safety at reduced costs. One such technique is diagnosis. Diagnosis in general is a term that includes several research and application fields. Examples of such fields, that are technology drivers, are the fields of supervision both on-line (on-board) and off-line (on ground), operator support that evolved from the Harrisburg accident, and law based emission diagnostics regulation e.g. as stipulated by *California Air Resource Board* (CARB).

The current work is an investigation in the cross field between safety assessment and diagnosis techniques. The first step was to root the work in existing safety practice. This means that the Swedish defense procedure has been adopted as described in *H SystSäk E*. It is a safety framework that uses fault tree analysis and failure mode effect analysis as important tools. Thereafter some flight applications were investigated together with Saab specialists to capture and formulate some aspects that are non-trivial to cast in the existing safety framework. Examples of such aspects found are for instance related to performance requirements in different operational model. A principle case study was then formulated using laboratory equipment, with the aim to capture some of the identified aspects in the problem formulation. A complete process for safety analysis was then completed along the lines of *H SystSäk E* including all meetings and documents required therein. Several observations were done during this work, but the overall conclusion so far is that the effect of introducing diagnosis algorithms can be handled in the safety analysis, and, yes, that there is a promise that diagnosis algorithms can improve safety in a structured quantitative way by lowering the contribution to the total failure risk from the subsystem being diagnosed.

Keywords: diagnosis, safety, fta, fmea

Contents

Chapter 1

Introduction

New demands from legislation, due to both higher demands on personal safety as well as higher emphasis on environmental demands, is forcing both small and large companies to put more and more attention towards supervision. However, diagnosis and supervision is still a highly diverse subject. There is a gap between the research being done in the academic world on safety and diagnosis questions and the methods that are presently carried out in the industry.

Saab has been interested in diagnosis for a long time, but also has a need for developing system safety and diagnosis issues further in the future. In this co-project the departments of saab that are involved are the ones dealing with safety problems surrounding their latest airplane, JAS 39 Gripen, and it is also a part of *Nationellt Flyg Forsknings Program* (NFFP). For JAS they have an extensive procedure at work already taking care of the process of guaranteeing a certain safety level (measured in number of flight crashes per flight hour). For the future, however, the numbers have to be decreased even further, especially considering the development of unmanned airplanes. That means that they, in a fairly short time, will have to develop their existing safety procedures in order to meet the new and increased demands. Therefore it is of high priority to investigate where and how much saab can benefit from the developments in diagnosis.

The group of Vehicular Systems at Linköpings universitet has had a growing diagnosis group, dealing with various problems concerning diagnosis and supervision, since 1996. The original problem was how to do diagnosis in vehicular systems, but the problems has since then grown in many diverse directions and the techniques now developed can be applied to a wide variety of diagnosis problems, arising in both technical and non-technical systems. By joining NFFP, this group gets insight in the existing safety practice and gets possibilities to see how diagnosis can be incorporated into this practice. Therefore it is highly beneficial to start a collaboration with a company such as saab, concerning the study of diagnostic problems.

This project is a first attempt of such a collaboration. It is about letting the diagnosis group at Vehicular Systems to get insight in how the system safety procedures are currently being done at saab, and what are saab's long-, and short-term needs for improvements in these systems. To make the objectives of this work a little more clear they are itemized in the next section.

1.1 Objectives

The main objectives of this report are the following:

1. Describe briefly how the safety procedures at saab are currently being done. This process is summarized in the first chapters of this report.

2. To do an abstraction of some of the most important safety aspects concerning airplanes.

3. Carry out the whole process used at saab for a example. For illustrative purposes a less complex example is chosen. For this principle case-study, determine in which steps the diagnosis methods of Vehicular Systems apply, and in what way.

4. Show how these diagnosis methods improve the safety aspects, both qualitatively and quantitatively, in the principle case-study.

5. Discuss how the results of the principle case-study can be generalized to full scale projects, and what new problems and possibilities there might appear by going to the full problem of constructing a safe manned or unmanned airplane.

1.2 Structure of the Report

The structure of the report is as follows.

Chapters 2 and 3 gives a background on safety concepts and safety procedures, and also how these are involved in characteristic subsystem. Both chapters are mainly based on information and presentation by saab specialists like Anna Karin Rosén and Predrag Pucar. Chapter 2 summarizes the basic concepts and methods used at saab at the moment, such as *Fault Tree Analysis* (FTA), *Failure Mode Effect Analysis* (FMEA). Further more, *Risk Priority Number* (RPN) and *severity number* are explained. Chapter 3 is more concerned with new navigation techniques and algorithms to be implemented in future generations of airplanes. The general ideas behind the new techniques are explained and their influence on safety is discussed. From the new navigation techniques, aspects that are difficult to include in the existing safety practice are extracted.

With these aspects given, a principle case-study is set up. The principle case-study is a slot car track extended with additional sensors and control possibilities. In Chapter 4 the slot car track and the connection to aircrafts are described. Furthermore, the specifications of the problem and the important features of the results are discussed. The results include many of the objectives specified in the previous subsection such as the answer to where the theoretical diagnosis tools might enter into the safety analysis, and also gives some simple quantitative and qualitative examples of how, and how much they can help the diagnosis task. The actual process of going through all the safety documents are however, due to their extensitivity, moved to an appendix. Finally in Chapter 5, the conclusions of the complete report are given.

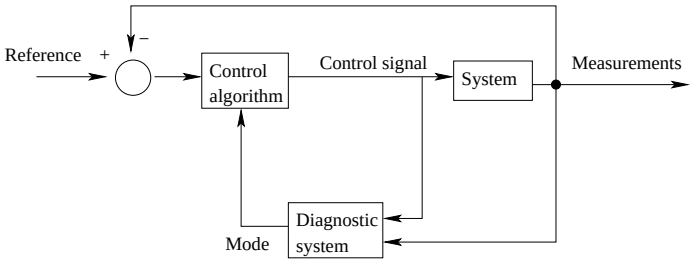


Figure 1.1: Schematic figure of a diagnostic system and how it's output can be fed back to the system to enhance its safety features.

1.3 Outlook

There are a number of different diagnosis methods that has the potential to enter into the saab processes (see e.g. (Nyberg & Frisk, 2003)). Here comes a brief outlook over some of them.

Passive FDI Methods

Fault Detection and Isolation (FDI) diagnostic systems can be used to monitor systems. The objective is to detect and isolate an upcoming hazard event before it reaches a critical stage. A passive FDI system does not itself excite the real system to obtain the information it desires, but uses only the natural input and output signals that arises from the ordinary working mode. In the principle case-study, explained later in the report, no such diagnostic systems have initially been implemented, and a major research question is what the benefits are of introducing a diagnosis system like the one shown in Figure 1.1. Another important question is how these benefits can be quantified. There might also be some safety drawbacks from introducing FDI methods in a system. In general, the safety features of the original system is altered when an FDI diagnosis system is introduced.

Active FDI Methods

In active diagnosis, the systems input is fully or partly controlled by the diagnostic system. That means that here the diagnosis system itself excites the system to get the signals it needs for its diagnosis work. Since this will reduce, to some degree, the functionality of the system it is mostly used in some safe modes, e.g. airplane in cruise mode or in on-ground mode. In connection with all FDI diagnosis systems, it is possible to detect degrading of system components, even though the system still provides functionality. This feature is, however, even more apparent for active diagnosis system.

To have an example of the benefits of these methods consider a rudder on an airplane before take-off. This is a safe mode to test the rudder with active diagnosis. One active diagnosis is that the pilot gives full rudder order and look at the rudder. If the rudder moves to end points then that functionality is given. It is however difficult for the pilot to asses the rudders response-time,

smoothness in movement etc. A full FDI diagnostic system would, however, be able to asses these facts.

Some Other Methods

Also other techniques are potential candidates when discussing design of diagnosis. Examples are formal methods, expert systems, and AI methods. One of the objectives of *formal methods* is to reduce the probability that faults in the software occur, another is to find faults in the software. Both faults built in to the software and faults caused by the interaction with the surrounding are considered. Formal methods is a diverse area but with the increasing use of software in almost all technical processes it is natural to keep developing it.

Expert systems is software that through interaction with the user, helps the user to state a diagnosis. With the increasing development in computer storage possibilities this is a method that may have increased potentials in the future.

Artificial Intelligence (AI) methods for diagnosis are mainly used to find discrete faults. AI diagnostic systems uses a database to search for faults in the system. It is possible to combine these methods with expert systems, where the user specifies faulty behaviors. The diagnostic systems use this extra information when searching for faults.

However, these other methods are not considered any further in this report.

Chapter 2

Safety and Diagnosis: A General Introduction

The first saab produced airplane J29 was produced in 660 specimen and 213 of them were lost. A later completed airplane project AJ/JA37 was produced in 329 specimen and out of those only 46 have been lost. The reason for this drastic improvement is that the security and safety of the airplanes has been emphasized more and more over the years. In this chapter we will consider the structure and methods of the existing safety work. We will give a small introduction to why failures occur, then look at some of the standards and requirements that presently is followed and finally give a brief introduction to evaluation techniques like for example preliminary hazard analysis and failure mode effect analysis.

2.1 Why Do Failures Occur

Failures can occur for many reasons. Here are some typical for a saab aircraft:

- Operating beyond design limits
- Operating limits were not clearly defined
- Vibration levels were higher than expected
- Temperatures higher/lower than expected
- Temperature change faster than expected
- Failure to anticipate how the customer would use the equipment
- Faults in development

2.2 Main Goal and Distribution of Responsibilities

Main goal

The aim of all safety analysis and safety system inclusions in an air plane is to be able to declare the air plane *airworthy*. According to TjF-FMV 197:47, 1997-

10-28 the definition of this is:

> **An air plane is *airworthy* if it is constructed, built, verified, equipped and maintained in such a way and has properties to fulfill the demands of safety.**

The achievement of this overall goal is distributed between a number of departments, but there are also a number of rules and working principles that those involved in the design process should follow. There are also extensive standards for how the safety aspects are included in the various parts of the work.

In General

For good *reliability*, design should consider:

- Use good praxis of design
- Simplify the design as far as possible
- Proceed in a conservative manner and use appropriate safety limits
- Use components and principles with known reliability
- Use known, tested, controlled and, as far as possible, non-critical processes

The principles for good *design* are:

- Eliminate hazards through design
- Minimize the effect so they can be controlled
- Introduce warning-system to make emergency procedures possible
- If it is impossible to eliminate or control a hazard - risks should be avoided through restriction, special instruction etc

Departments

There are several departments involved in the safety control of airplanes. One of them is *system safety and reliability* (Systemsäkerhet och Tillförlitlighet). The main obligations of this department are to:

- Identify and together with people in charge of design, construction, eliminate, minimize and control sources of risk, due to the *design solution* of the air plane.
- Leave information regarding the safety status, including possible risks, after design to the process of air-worthiness.
- Collect, analyze and transmit data regarding safety to people in charge of system safety, customers support and investments (choice of deliverer)

Standards for Reliability

There are several standards for system safety and reliability, both international and national. Among the most important are MIL-STD (MIL standard), MIL-HDBK (MIL handbook), SIS (Standeriseringskommisionen i Sverige), IEC (International Electrotechnical Commission).

2.3 Reliability Analysis

Reliability is the duration or probability of a failure-free performance under stated conditions. The purposes of reliability analysis are to:

- Compare reliability and safety aspects of different system design solutions
- Calculate probability measures regarding e.g. mission reliability
- Make maintenance analysis
- Make safety evaluations
- Make safety analysis

Reliability analyses are techniques for working with some of these items. Depending on the application, there are variants of reliability measures, e.g. *mission reliability*. It is defined as the measure of the ability of an item to perform its required function for the duration of a specified mission profile. Mission reliability defines the probability that the system will not fail to complete the mission, considering all modes.

2.4 Reliability Analysis Methods

There are many methods for evaluating the nature and origin of faults and hazards. These will be discussed in detail in the coming sections.

PHL and PHA

Preliminary Hazard List (PHL) is a list of all possible hazards identified with respect to aircraft, occupational, third party, environment and occupational health hazards. At this point it is desired to find *all* of them, regardless if they are unimportant/impossible or not. The PHL is written early in the development program to influence the design as early as possible. The PHL is a basis for a *Hazard log*. The hazard log is a record of all collected information about each hazard.

A *Preliminary Hazard Analysis* (PHA) is a detailed analysis of all hazards in the PHL. Here each hazard is named and classified in degree of severity. The effect and possible causes of each hazard is also given. The purpose of PHA is to identify safety critical subsystems, functions and equipment affected, provide an initial assessment of the hazards, and recommend actions which may be necessary in order to eliminate identified hazards or control the hazard risk to acceptable level. Since a PHA starts at the *hazard* and then determines

the possible faults that might have caused the hazard, it is called a *top-down* approach.

Failure Mode Effect Analysis

To be able to describe what *Failure Mode Effect Analysis* (FMEA) is, we will first explain the concepts failure, failure mode and effect of a failure. A *failure* is the event, or inoperable state, in which any item or part of an item does not, or would not, perform as previously specified. Examples of failures are *broken* and *worn*. *Failure mode* is the consequence of a mechanism through which a failure occurs, i.e. leakage and open circuit. Finally, the *effect of failure* is the consequence of a failure. It is the effect of the failure that will define the severity.

FMEA is an engineering technique used to define, identify, and eliminate known and potential failures, problems, errors and so on from the system, design, process and service, before they reaches the customer. For each failure, an estimate is made of its effect of the total system, i.e. a bottom-up method. To minimize the problems for the customer, it is important to treat the most important problems. The importance of a problem i.e the priority, is estimated with the *risk priority number* (RPN). The RPN is the product of frequency of occurrence, severity, and detection. *Occurrence* is the frequency of the failure. *Severity* is the seriousness effect of the failure. *Detection* is the ability to detect the failure before it reaches the customer. A good FMEA

- identifies known and potential failure modes,
- identifies causes and effects of each failure mode,
- prioritizes the identified failure modes according to the RPN, and
- provides a corrective action from problem follow-up.

A FMEA form generally consists of the following parts:

- System name
- System responsibility (e.g. an organization)
- Person responsibility
- Involvement of others inside the organization
- Supplier involvement outside the organization
- Model or product
- Engineering release date of the system
- Prepared by the design engineer of system
- FMEA initiation date
- FMEA revision date

The FMEA form also includes a table which usually contains the categories shown in Table 2.1.

Different Versions of FMEA

An extension of FMEA is *Failure Mode Effect and Criticality Analysis* (FMECA) where also the *criticality* of each failure mode is considered. *Criticality* is a relative measure of the consequence and frequency of occurrence of a failure

Table 2.1: FMEA form

Category	Subcategory	Responsibility
System function Potential failure mode		Engineer ”
Severity	Potential effects of failure Critical characteristics Severity of effect	Engineer and team Team ”
Occurrence	Potential causes of failure Occurrence number	” ”
Detection	Detection method Detection number	” ”
RPN		”
Action	Recommended action Responsiblity and completion date Action taken	Engineer with selective team ”
New risk analysis	Severity number Occurrency number Detection number RPN	” ” ” ”

mode. At saab the following facts should be given for each failure mode: mission phase, failure rate, primary failure effect, aircraft and mission failure effect, criticality, detectability, and compensating factors. Another version of an FMEA is a *functional FMEA* (FFMEA), which identifies possible causes for losing a function.

Fault Tree Analysis

Fault Tree Analysis (FTA) is a top-down deductive analytical technique of reliability and safety analysis. The purpose of FTA is to identify which subordinate events, or combinations of events, that can cause undesired events. When the causes have been identified, the corrective actions required to prevent or control the causes need to be determined. The FTA is also used to calculate failure probabilities. A fault tree is a model that logically and graphically represents the various combinations of possible events, both faulty and normal, occurring in a system that leads to the undesired top event. The tree show the cause and effect relationships between a single, undesired event (failure, hazard) and various contributing causes. Usually probilities are associated with the failures.

Failure Mode Effect Test

Failure Mode Effect Test (FMET) is classified as a *bottom up* approach. Here a fault is physically introduced and then its effects are analyzed. This method is applied to all critical systems, like for example the control system.

Table 2.2: Frequency classification

Name	Definition[10^{-6}]	Risk level	Description
Frequent	> 1000	6	Continuously experienced
Probable	> 100	5	Will occur frequently
Occasional	> 10	4	Will occur several times
Remote	≈ 1	3	Unlikely but can reasonably be expected to occur
Not excluded	< 0.1	2	Unlikely to occur but possible
Improbable	< 0.01	1	Will not occur

Table 2.3: Hazard category definition

Name	Definition	Risk Level	Description in general
Catastrophic	$\frac{1}{1} - \frac{1}{10}$	4	The event will result in dead or severe bodily injury or severe material damage.
Critical	$\frac{1}{10} - \frac{1}{100}$	3	The event results in bodily injury or major material damage or require immediate countermeasure to avoid that the above occurs.
Marginal	$\frac{1}{100} - \frac{1}{1000}$	2	The event can in the general case be controlled but bodily injury or material damage can not be excluded.
Neglecteble	$< \frac{1}{1000}$	1	In normal cases the event will not lead to any bodily injury or material damage.

2.5 Risk Assessments

Risk assessments are used to decide work-priority and aircraft air-worthiness. A specific event is classified in two parts, frequency of event and hazard category of event. Risk assessment for a given event is the frequency of event times the hazard category of event.

Frequency of event is measured as number of occurred events per flight hour and is classified in Table 2.2.

Hazard category of event is measured as number of “complete plane crash” per occurred event and is classified in Table 2.3.

From the classification of an event into frequency and hazard, the *risk* is defined as *risk level of frequency* times *risk level of hazard category*.

The risk for an event is used to asses if the risk level of frequency or risk level of hazard category have to be reduced due to air-worthiness and / or customer demands. The classification used in (Wiktorin & Ekholm, 1996*b*) is given in compact form in Table 2.4.

Table 2.4: Risk assessment.

Importance	Description
16–24	Intolerable risk
8–15	Limited tolerable risk
1–7	Tolerable risk

Table 2.5: Example: Accident risk contribution budget

Accident type	Accident rate
Aerodynamic material group	1%
Landing gear material group	2%
Engine material group	10%
⋮	
Sum material groups	25%
Unanticipated technical failures	25%
Other reasons (e.g. pilot)	50%
Grand total	100%

2.6 Accident Risk Contribution

To estimate and control accident risks, saab uses an accident contribution system. Accident rate is defined as the mean value of aircrafts lost during service per 10^5 flight hours. The accident risk contribution is by saab defined as hazard category times probability.

The accident rate is divided in two different types of accidents. The accident rate is first divided equal between *technical failures* and *other failures*, e.g. failures caused by pilot. The technical failures are divided approximately equal between *material groups* and *unanticipated technical failures*, e.g. see Table 2.5. Each material group must then ensure that the accident risk contribution for their group is not exceeded.

2.7 References

For general information about safety and reliability see (Villemeur, 1992*a*) and (Villemeur, 1992*b*).

Fault tree analysis is studied in more detail in (Stamatelatos & Vesley, 2002) from U.S. NASA and (Vesley, Goldberg, Roberts & Haasl, 1981) from the U.S. nuclear agency.

The Swedish safety standard is described in (Wiktorin & Ekholm, 1996*b*; Wiktorin & Ekholm, 1996*a*). Guidelines for safety assessments in civil airborne systems is given in (SAE, 1996)

2.8 Summary

Two common reasons for aircraft failures are that faults in the development were not corrected and that the aircraft is operating beyond design limits. The

probability for failures, e.g. caused by these two reasons, can be reduced by a systematic safety analysis.

The process of finding all possible faults that can become a failure relies on the ability of engineers to predict possible situations. To be able to predict possible situations, detailed system knowledge is required. Since no engineer is an expert on the entire aircraft, many experts on different subsystems and from different departments must be involved. In addition to exhaustive safety analysis of each subsystem, the interaction between subsystems and between the aircraft and its environment must be analyzed.

To organize and simplify the extremely difficult analysis process, the process needs to be extensively documented and systematically performed. The Swedish defense procedure is described in *H SystSäk E* (Wiktorin & Ekholm, 1996*a*).

Two important goals of safety analysis are to reduce the accident rate to an acceptable level and to justify the estimation of the accident rate. Important tools for estimation of the accident rate and analyzing system safety are fault tree analysis and failure mode effect analysis.

Chapter 3

Problems and Challenges around Advanced Navigation Systems

In this chapter a new navigation and landing system is presented. The goal of this chapter is to describe safety aspects that are difficult to include in the existing safety framework. These aspects are identified together with saab specialists.

3.1 Introduction

This chapter has its roots in a presentation given by Predrag Pucar on the topic of *Problems and challenges around NINS/NILS*.

The development of *New Inertia Navigation System* (NINS) and *Navigation Instrumental Landing System* (NILS) is carried out by saab Gripen development and saab Dynamics AB and is supported by *Försvarets Materialverk* (FMV).

The goal of the project is to develop a landing system using only existing sensors. The landing system shall be certified for CAT I[1] landing. The system shall benefit from navigation information supplied from infrastructure systems, if available.

3.2 Equipment

A part of the project description is that only existing sensors should be used. Some of these sensors are given on the picture in Figure 3.1. Here follows a short description of some of the components:

- *Inertia Navigation System* (INS) uses a gyroscope to estimate the position and positional change of the airplane.

[1] ILS Cat 1 – Cloud Base: 200 feet above ground level, minimum visibility: 550 meters

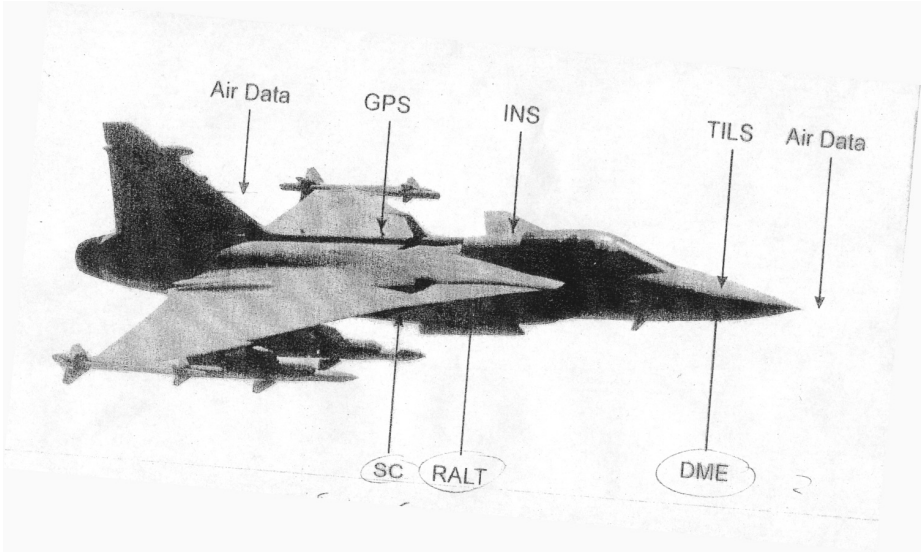


Figure 3.1: The most important sensors on a JAS 39 Gripen.

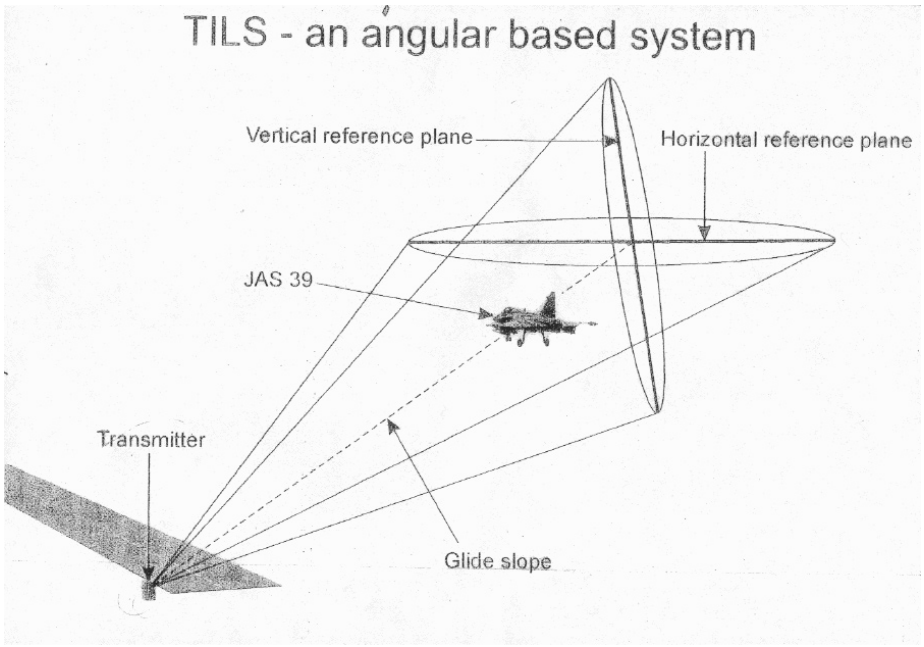


Figure 3.2: The basic principles behind TILS.

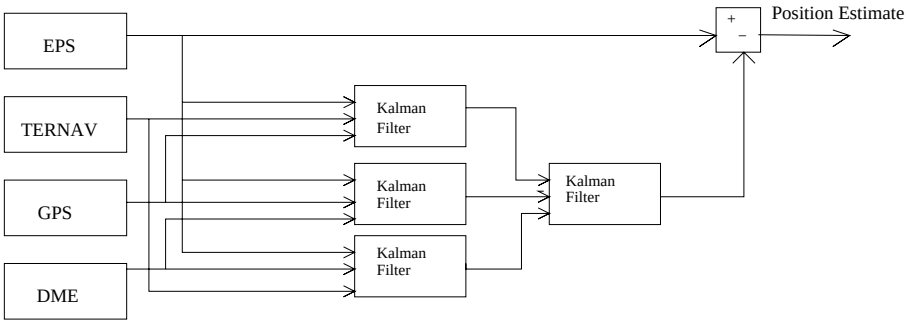


Figure 3.3: Generalized observer model of decentralized Kalman filter.

- *Tactical Instrumental Landing System* (TILS) is an angular based system which utilizes the signal from a ground positioned transmitter (see Figure 3.2).
- *System Computer* (SC).
- *Global Positioning System* (GPS) is situated on the top of the airplane. This information together with the estimate of the distance from the ground transmitters (from the box denoted DME in Figure 3.3), and the position estimate of the *terrain navigation* system (TERNAV) are fed to a Kalman filter (see Figure 3.3).
- *RALT* measures the altitude of the airplane. This information is used in the TERNAV (see Figure 3.4).

3.3 Methods

In Present Use

The instrumental landing system at present use is called *tactical instrumental landing system* (TILS). TILS is an angular based system and it utilizes the signal from a ground positioned transmitter. A schematic drawing of its use is given in Figure 3.2.

New Inertia Navigation System (NINS) and New Instrumental Landing System (NILS)

The systems, NINS and NILS are new, and in addition to TILS, NINS and NILS also include TERNAV. The new systems require no new sensors so the improved positional estimation, which is the goal, is accomplished only through new software and algorithms. A high-level block diagram of NINS is shown in Figure 3.4 and the idea of the observer model is shown in Figure 3.3. In these two figures, it is clear that the basic idea is to combine different estimates of position and velocity to achieve an improved estimate. Since one new independent position estimate is introduced with TERNAV, faults in one of the sensors or estimates are handled in a more robust way.

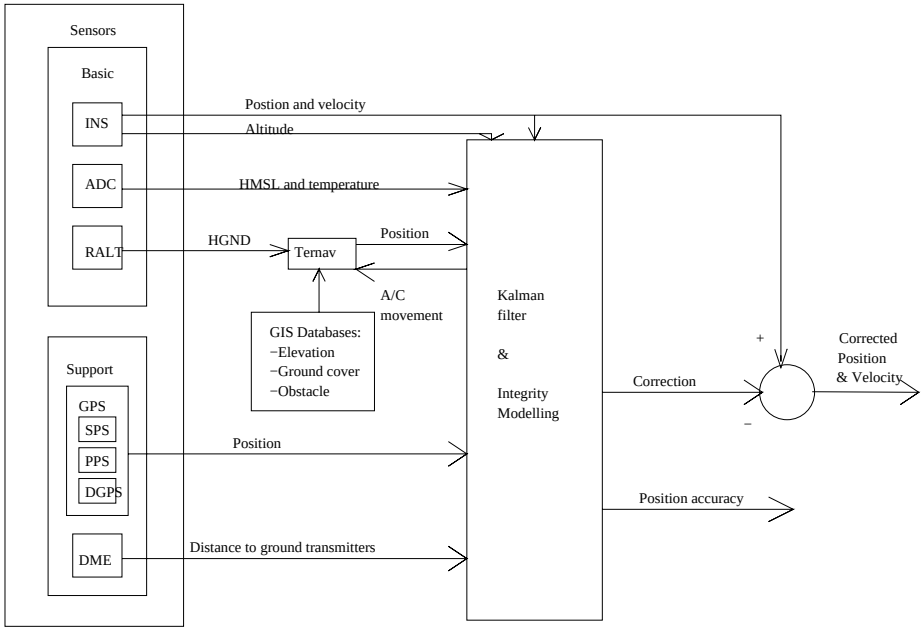


Figure 3.4: High-level block diagram of NINS.

Some of the advantages of NINS / NILS, will be:

- Superior Navigation Accuracy
  - Achieves Military GPS Performance
  - Impossible to jam
- Aircraft Autonomous Landing Capability
  - Neither costly infrastructure nor special aircraft equipment needed
  - IMC landing capability on austere bases
- More flexible tactical behavior
  - Enhanced weapon delivery capability
  - Improved random route navigation

Another important new feature of the NINS is the *Terräng Navigering* (TERNAV) principle which is described in the next section.

The TERNAV Principle

One of the new features of the NINS is the usage of a large database called *Geographic Information System* (GIS). It contains information of the the terrain elevation and all man made obstacles in a grid system. The database contains information of what kind of vegetation is on the ground and has a resolution of 50 meters between the points. The uncertainty is about 2.5 meter.

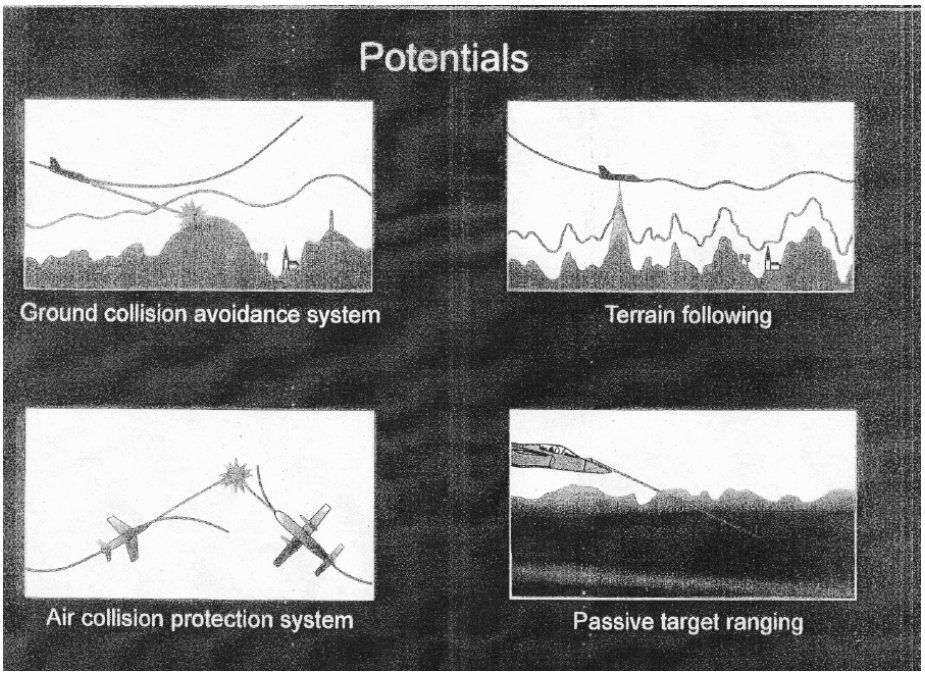


Figure 3.5: The potentials with the new Navigation system.

In addition to existing position estimates, an additional position estimate is obtained using a point mass filter combining the terrain elevation information from GIS and the altitude estimate given from the RALT-sensor (see Figure 3.1). The method, however, is based on variations in the terrain and does not function as well over flat areas or over water.

3.4 Future Potentials

Some of the potentials with the new Navigation systems are (see also Figure 3.5):

- Ground collision avoidance system
- Terrain following
- Air collision protection system
- Passive target ranging

3.5 Conclusions

NINS / NILS contains safety aspects that are difficult to include in the existing safety framework. In Figure 3.5, terrain following is one example of an operation that is more risky than flying at high altitude. Hence the accident rate depends on the operation of the aircraft.

A second example is that environmental conditions influence. An obvious example is different weather conditions, but there are several others, e.g., the accuracy of the terrain navigation system is high when flying over rough terrain compared to flying over a flat sea.

Another difficult safety aspect is that NINS / NILS take measurements from the environment. It is difficult to predict all possible measurements that can appear and the result of the corresponding control action. Thus, the outcome of the control action influence the accident rate, also when the control algorithm is working exactly as specified.

Moreover, if the system only is used as an alarm system, then the pilot action must be predicted to be able to calculate the influence on the accident rate.

To conclude this chapter, human interaction, environment interaction, and intended use of the aircraft are factors that are difficult to include in the existing safety framework. However these factors are important to consider, because they influence the accident rate.

Chapter 4

Analysis of a Principle Case Study

It is necessary for a company to show that an airplane is air-worthy to get a flight permission. The air-worthiness is based on the accident rate, defined as the probability of a plane crash per flight hour. If the company can show that this rate is lower than a given statuary number, a flight permission can be given. To support this given rate, the company is obligated to do an extensive safety analysis of the aircraft.

Since the accident rate and the safety analysis to support this number are significant for the aircraft industry, we performed a safety analysis of a principle case study. The case study chosen is a computer controlled slot car track where similar features as those for aircrafts can be identified.

4.1 Objectives

The objectives of the case study are:

- To gain a deeper knowledge of how system safety activities are performed according to *Försvarets Materielverk* (FMVs) instructions and directives.

  The safety regulations are specified in (Wiktorin & Ekholm, 1996*a*), which is the handbook in system safety for the Swedish Armed Forces. (More information in Section 4.5.)

- To understand the underlying process of the safety activities, and the relation between the research on diagnostic methods conducted at Vehicular Systems and system safety.

4.2 Similarities between the Slot Car Track and Aircrafts

To make a safety analysis of the slot car track interesting in a flight safety aspect, it was crucial that the slot car track case had similar important aspects as the aircraft case. Some of these aspects are discussed below.

The probability of a plane crash per flight hour is for the slot car track the probability of a car leaving the track per drive hour, i.e. the accident rate for the slot car track. It is important to specify the intended use, to be able to calculate an accident rate. For example if the car only stands still, the probability of a car leaving the track per drive hour is zero (if some specific human-related factors are ignored.). Therefore speed performance requirements were added. These speed performance requirements correspond to mission demands and operation limits for aircrafts.

Control software in aircrafts is safety critical and needs to be carefully analyzed to get the crash probability contribution. In aircrafts, software is used for control, and to include the software aspect into the slot car track project, the cars are also controlled by software. There are two possibilities to drive the cars, either by an auto-pilot, or by the user giving the input to the software, which carries out the order.

On the track, there are position sensors that can be used for auto-pilot steering. Therefore, the principle case study also captures the impact of safety when actuators and sensors fail on the aircraft.

As for aircrafts, a human is involved in the operation of the system. It is interesting to learn how human mistakes are taken into account in the crash probability contribution. There can be many different causes that lead to a crash, e.g. the user has not been given proper education of the system, or that the system has not been correctly designed.

Another aspect that is not directly related to the calculation of the probability of a plane crash per flight hour, but still is important, is how safety is handled during the design of the aircraft. During the development of, e.g. the auto-pilot software, it is important to follow a safety plan to reduce the crash probabilities during the testing phase.

We find that many important safety aspects involving aircrafts air-worthiness have direct correspondence to safety aspects of the principle case study. Therefore knowledge gained in the case study can be interpreted in the context of safety analysis of aircrafts.

4.3 Case Study Description

In Vehicular Systems laboratory, a 20 m slot car track (bilbana) has been constructed, see Figure 4.1. The track is equipped with 10 sensor units for car detection and is computer controlled. The voltage supply is fully controlled, e.g. from matlab. The track is being used for an introduction course in automatic control, given for first year students at the under graduate program in Applied Physics and Electrical Engineering (Y). The objective is to control the car lap time to a given reference time.

The system consists of:

- 20 m slot car double-track.
- 10 sensor units. The sensor units have phase-modulated IR diodes and sensors. The diodes and sensors are connected to an analog filter and communication unit.
- One or two slot cars.

Figure 4.1: Slot car track at Vehicular Systems, including sensors and control system.

- Voltage supply unit.
- Electronic control box connected to computer I/O-card, sensor units, voltage supply and tracks. The box handles communication to I/O-card and control the voltage supply to the tracks.
- Computer with I/O-card for communication with the electronic control box.
- The system is placed in a room with furnishing and glass windows.
- Software. The software consists of:
  - Low-level software for I/O-card communication.
  - High-level software consisting of control algorithm, log and diagnostic software, display control and post-race log treatment.
  - Software from external suppliers, Matlab, labview, windows etc.

4.4 Time Line

The case study was started 11th June 2002 and finished 3rd February 2003. For further details see Appendix 1.

4.5 Safety Regulations

In this section an introduction to the safety regulations specified in (Wiktorin & Ekholm, 1996*a*) are given.

Below is a short description of the documents to be produced and the various activities that shall be performed.

UTTEM – Safety requirements in TTFO Specification of safety requirements to be included in the overall system requirements (the TTFO).

RFP – Request for Proposal Converts the safety specification specified in UTTEM into a form that is suited for use when submitting a tender.

SSPP – System Safety Program Plan To determine contractual system safety obligations during the material's development and manufacture stages.

SSWG – System Safety Working Group The purpose of the safety group is to support the development of safety-critical systems. Should consist of members from orderer, vendor and end-users.

SSPR – System Safety Progress Review To ensure that the system safety program plan (SSPP) is followed and to decide on risk-reducing measures as per the safety analyses (SHA / SSHA), (O&SHA / EHA).

SRP – Safety Requirements Proposal To formulate the safety requirements into a main specification and a sub-system specification valid during the product development phase, and whose contents are verified at the end of the development phase.

PHL – Preliminary Hazard List Purpose is to identify hazards and the hazard events they may possibly cause.

PHA – Preliminary Hazard Analysis To identify and document hazards and identify related hazard events. Based on preliminary hazard list (PHL).

SRCA – Safety Requirements/Criteria Analysis To identify safety requirements relevant to the system, and to use such sources as the preliminary hazard list (PHL) and preliminary hazard analysis (PHA) to state the safety requirements that are to be included in the system's requirement specifications.

SHA/SSHA – Sub System Hazard Analysis To identify hazard events and assess their functional risks. Preliminary for the entire system and interaction between sub-systems (SHA), and for sub-systems and their components (SSHA). Tools such as FMEA and FTA are used in the analysis.

O&SHA – Operating and Support Hazard Analysis To asses the hazards involved in operating and support and to asses whether operational and maintenance procedures are sufficient to eliminate, control or reduce identified faults and hazards. Tools such as event tree analysis can be used.

EHA – Environmental Hazard Analysis Similar to O&SHA but for environmental hazards.

TES – Test and Evaluation To specify those activities that are necessary for testing the system in cases where there is a risk for personal injury or damage to property or the external environment. SAR and SCA can be used to evaluate test suitability.

SRS – Safety Verification To specify the design measures needed to prevent faulty handling of the system.

FRACAS – Failure Reporting, Analysis and Corrective Action System Provides feedback about safety-related information to those responsible for improving system safety.

SV – Safety Verification To asses whether the safety requirements that are applied to the system have been verified. Input data for this is safety requirements (SRP), safety requirement analysis (SRCA), failure reporting (FRACAS), etc.

SCA – Safety Compliance Assessment The producers opinion about the systems safety.

PHST – Package, Handling, Storage and Transport Regulation Safety requirements for users who comes in contact with the system in package, handling, storage or transport.

SS – Safety Statement Formally approve the safety of the system.

TSR – Training Safety Regulations Safety requirements when using the system for training.

SR – Safety Release Formal decision about the use of the system.

RADS – Risk Assessment at Disposal of Systems To provide a basis for risk assessment when system disposal is under consideration.

By following these instructions the hazards that is associated to the system are reduced.

4.6 Restrictions

According to FMV's system safety instructions, several safety analyzes, using FMEA, FTA, etc., shall be performed, see e.g. SHA. These shall be performed for different parts of the system and with respect to different hazards. Since these are performed with the same methods, it was decided that for our principle case study, only one safety analysis should be performed. The safety analysis is performed for track, car and control system and where applicable, notably FTA, with focus on the hazard "car off-track".

Further studies of FTA with top events such as: Broken window; Personal injury caused by broken window; Personal injury caused by direct hit by car; etc., should be performed to gain a complete safety analysis.

4.7 Safety Activities in Principle Case Study

All documentation from the case study are included in Appendix 1. It includes reports from the activities which leads to the *Safety Release* (SR). Below is a short review of some of the documents.

UTTEM – Safety requirements in TTFO See document.

RFP – Request for Proposal In the RFP, safety specifications are stipulated. The overall product specifications have already been stated in a different project. Therefore, the RFP is based on this, but with additional safety specifications.

SSPP – System Safety Program Plan See document.

SSWG – System Safety Working Group The group consists of the authors to this document, and some people with in-depth knowledge about the system.

SSPR – System Safety Progress Review See document.

SRP – Safety Requirements Proposal See document.

PHL – Preliminary Hazard List A preliminary hazard list is constructed. It was constructed by the authors to the PHL document, with support from the SSWG.

PHA – Preliminary Hazard Analysis The hazards stated in PHL is studied in more detail. They are given a consequences rating, which are divided into four degrees.

SRCA – Safety Requirements/Criteria Analysis Not performed in the case study.

SHA/SSHA – Sub System Hazard Analysis In the SHA document, some of the hazards found in the PHL is studied in detail. The FMEA is performed for the overall system while only the hazard “car off-track” is studied in detail with FTA. For more information about the restriction see Section 4.6 in this document.

In Section 4 in the SHA-document, the FMEA analysis is presented. The risk priority number is calculated as frequency times consequence. A low risk priority number stipulates a serious hazard. It can be seen that the most serious hazards are, faulty in-data, and faults in the control algorithms. Both these hazards have the result that the car goes off-track. This is the reason why it is the “car off-track” hazard that is studied in the FTA analysis.

In Section 5 in SHA, the FTA analysis is presented. It can be seen that it is predicted that the car will go off-track about 5.08 times per hour.

O&SHA – Operating and Support Hazard Analysis Not performed in the case study, see Section 4.6.

EHA – Environmental Hazard Analysis Not performed in the case study, see Section 4.6.

TES – Test and Evaluation In the document, the safety regulations that should be followed when testing the system is specified.

SRS – Safety Verification See document.

FRACAS – Failure Reporting, Analysis and Corrective Action System The FRACAS is described in the document.

SV – Safety Verification The document shows that required safety activities have been performed. The safety regulations have been implemented.

SCA – Safety Compliance Assessment In the document the producer states that the slot car track fulfills the safety requirements. It is described how this have been achieved.

SAR – Safety Assessment Report No specific document. See SCA above.

PHST – Package, Handling, Storage and Transport Regulation Safety requirements for use, service, and transport, is stipulated in the document.

SS – Safety Statement Formally approve the safety of the system. The SSWG have been consulted before the system was approved.

TSR – Training Safety Regulations See document.

SR – Safety Release It is stated that the use of the system can start.

RADS – Risk Assessment at Disposal of Systems see Document.

4.8 Safety Results

The case study has found that the system fulfills the safety requirements, see *Safety Statment* (SS) in Appendix 1. Safety restrictions during handling are found in the *Safety Restrictions* (SRS) document. To provide feedback about safety-related events, the *Failure Reporting, Analysis and Corrective Action System* (FRACAS) shall be followed at all times. It is found in the documentation.

Even though the system has been found to fulfill the safety requirements the system can be made safer. From the *System Safety Analyses* (SHA) it is concluded that the car will go off-track 5.08 times for each hour of use[1]. A review of the FTA shows that the majority of this hazard is emerging from the control algorithm (2.5), missed check-point detection (1.0), and the in-data supplied by the user (0.63). The high number for the control algorithm is mainly from the cases when the reference time is close to the minimally possible time, see SHA. If these numbers were reduced the system overall safety would greatly increase.

Formal methods could be used to reduce the number of faults caused by the software, e.g. from faulty control algorithms.

A review of the FMEA show that the hazards with most severe consequence are faulty in-data from the user and other faults that can cause maximum boost. If also frequency is considered, i.e. the RPN number, it is shown that in-data from user and the control algorithm are the main hazards.

[1] This have partially been verified through use of the system.

4.9 Gedanken Experiment

To lower the hazard, "car off-track", it is possible to use the methods discussed in Section 1.3. In this section a gedanken[2] experiment will be used to show how the hazard can be reduced.

In Section 4.8 it was stated that the majority of the hazard is emerged from three parts, the control algorithm, missed detection, and in-data from user. Since these three parts is responsible for 4.13 of the total number 5.08, the experiment will try to lower these three.

Control Algorithm

In the SHA it was stated that the control algorithm might be badly implemented. Stability has not been shown and limitations on boost have not been introduced. One of the major causes to the hazard car off-track, is caused by faults in the control algorithm which results in unreasonable high boost. To reduce the hazard, a low-level boost supervisor will be introduced. Since it is built into the system at a low-level, it will handle all unreasonable boost levels from the high-level software.

It is predicted that 75% of the faults will be handled by this new software. Since this is a gedanken experiment, this number is not supported by experiments and statistical data. It is rather based on experience, reasoning and consultation with the *System Safety Work Group* (SSWG).

Missed Check-point Detection

A missed check-point detection can be caused by the car skidding, bad reflection causing the sensor to get a bad signal, etc. The check-points are used to decide if the car is on a curly or straight part of the track, and thereby which boost should be used. So if a check-point is missed this might cause a too high boost on a curly part which leads to the car goes off-track.

To reduce this hazard a *Fault Detection and Isolation* (FDI) diagnostic system is recommended. A model of the car and track would give an approximation of the correct position of the car. The model would be feed with the same boost signal as is sent to the hardware, and the check-point detections are used as feedback. If a check-point is missed this could be detected and a warning issued. The warning can then, for example, be sent to the control algorithm which takes appropriate measures.

It is predicted that 95% of the faults will be handled by this new software. This number is also based on experience, reasoning and consultation with the SSWG.

Note: Even though the software presented will handle a majority of the faults, it might also introduce new faults. If for example the car slows down in some part of the track and then continues as normal, there is a risk that the diagnostic system issues a warning that a check-point have been missed. The result might be that the control algorithm increases the boost and the car goes off-track. These faults should not be ignored.

[2] A gedanken experiment is a thought experiment, i.e. an experiment that is run in the mind.

There are some ongoing research on this subject, it will be presented in (Holmstrand, 2003).

In-data From User

If the user supplies the system with a faulty reference-time, the car might go off-track. A faulty reference-time is an unreasonable short reference-time or an unreasonable long reference-time. An unreasonable short time is a time that is impossible for the system to handle. The car will definitely go off-track. The result of an unreasonable long time is more difficult to judge. The cars have a relatively high static friction which means that it is difficult for the control algorithm to drive slowly. The car might stop in some part of the track, and to get it going again the control algorithm have to increase the boost when the car does not arrive at the next check-point. This might cause the car to go to a high speed, when it starts to move again after the stop. The result might be that the car goes off-track.

To reduce this hazard a model for reasonable reference-times will be constructed. But, only too short reference-times will be supervised.

It is predicted that only 50% of the faults will be handled by this new software. This is based on experience, reasoning and consultation with the SSWG.

Result of New Software

The three most severe parts of the hazard “car off-track” has been reduced.

The new fault tree is shown in Figure 4.2. The tree is based on the fault tree in Section 4 of the SHA documentation. The leafs have been found by experiments, consultation of data from suppliers, and reasoning in the SSWG.

As can be seen in the figure, the probability for the hazard has been reduced to 2.07. This is a large decrease compared to the former probability of 5.08.

4.10 Conclusions

A principle case study has been analyzed for safety. The work has followed *H SystSäk E*, the safety-standard for the Swedish armed forces. The safety activities leading to the safety statement have been described.

It has been shown that different diagnostic/supervision systems can be used to lower the hazards.

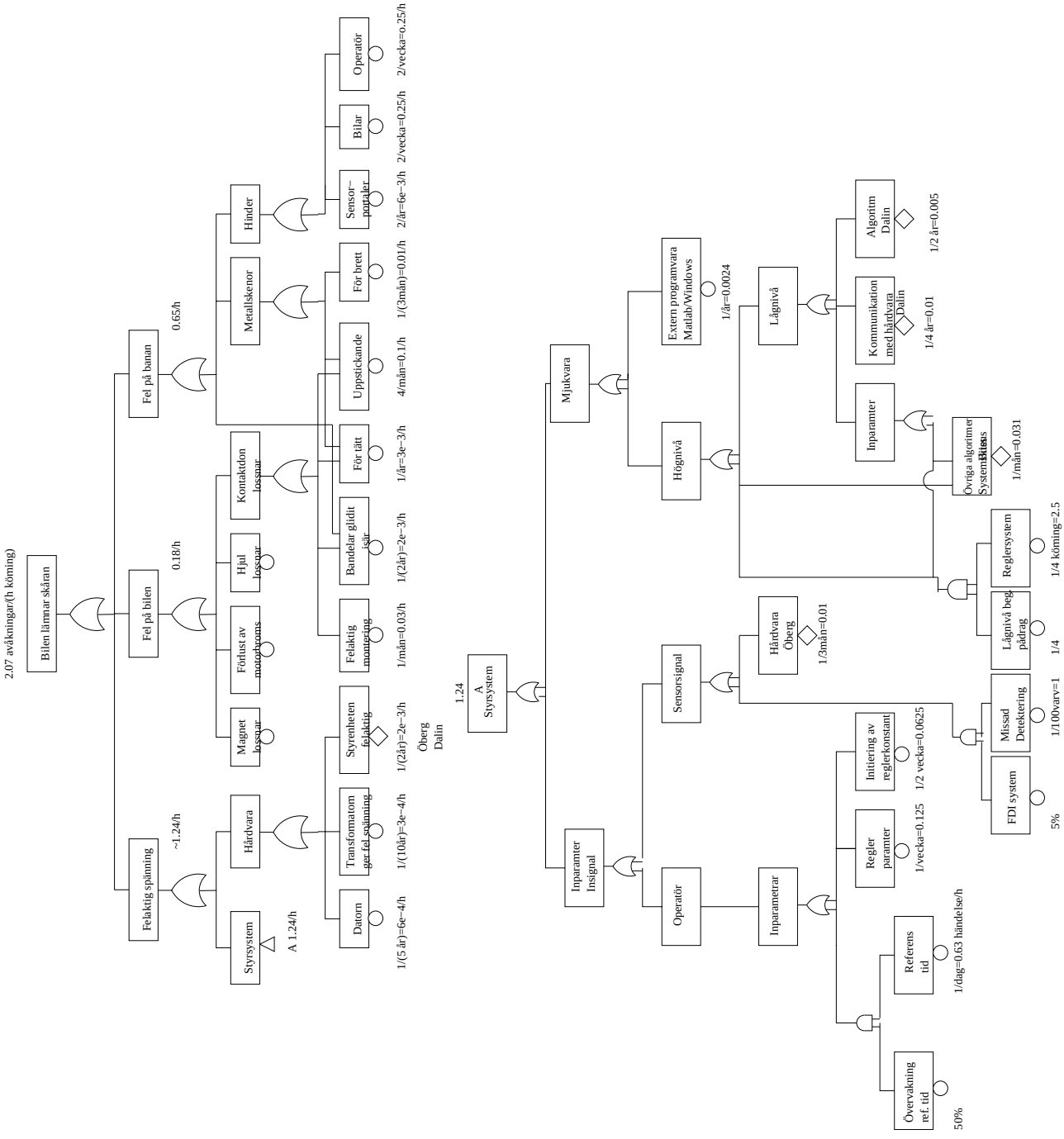


Figure 4.2: Fault tree with new software

Chapter 5

Conclusions

A study of the methods for system safety currently in use in the design process at saab-aircraft has been made. The main features of these methods have been described in this report. Two main objectives of this study are to identify aspects that are non-trivial to cast in the existing safety framework and to see where the scientific method of model based diagnosis enters. Some of the conclusions of this work are:

- Producing all the documents in the safety analysis process is highly time-consuming and also contains many openings for mistakes. To remedy this, the process needs to be as systematic as possible. Many documents depends on other documents, e.g. if a hazard is identified, it is included in PHL and analyzed in PHA, thereafter, the corresponding failure is analyzed in a FTA. Therefore it is recommended to have a computer program that supervises and makes sure that all documents are updated after adding more information in some document, e.g. a new hazard in the PHL.

- Human interaction, environment interaction, and intended use of the aircraft are factors that are difficult to include in the existing safety framework. However these factors are important to consider, because they influence the accident rate.

- It has been shown in the slot car case study that if for example a leaf of a fault tree contributes unacceptably much to the accident rate, then model based diagnosis enters with the potential to lower the rate- and seriousness-numbers in this leaf and therefore also with the potential to lower the accident rate.

- When model based diagnosis together with a recovery action reduce the accident rate, then diagnosis is an alternative to e.g. introducing hardware redundancy.

- By only using simple models it is possible to construct simple test quantities that together with a recovery action can significantly decrease the accident rate. For the slot car track, the test quantity $T_{slip} :=$ *Given velocity - measured (or estimated) velocity*, can easily be constructed, and once this

is constructed e.g. structured hypothesis tests are applicable (Nyberg & Frisk, 2003).

- During safe operation, e.g. before take-off, also active model-based diagnosis, in addition to passive diagnosis, can be used to reduce probabilities of failures. The probabilities are reduced because faults can be detected and attended to before the aircraft operates in working points where the fault becomes a failure.

Bibliography

Holmstrand, A. (2003), System safety effects caused by diagnostic systems, Master's thesis, Linköpings Universitet, SE-581 83 Linköping.

Nyberg, M. & Frisk, E. (2003), *Diagnosis of Technical Processes*, Linköpings Universitet.

SAE, ed. (1996), *Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment*, SAE. American National Standard.

Stamatelatos, M. & Vesley, W. (2002), Fault tree handbook with aerospace applications, Technical report, NASA, U.S.A.

Stamatis, D. (1995), *Failure Mode and Effect Analysis: FMEA from Theory to Execution*, ASQ Quality Press.

Vesley, W., Goldberg, Roberts & Haasl (1981), Fault tree handbook, Technical Report NUREG-0492, U.S. N.R.C., U.S.A.

Villemeur, A. (1992*a*), *Reliability, Availability, Maintainability and Safety Assessment Volume 1*, John Wiley & Sons.

Villemeur, A. (1992*b*), *Reliability, Availability, Maintainability and Safety Assessment Volume 2*, John Wiley & Sons.

Wiktorin, O. & Ekholm, R. (1996*a*), *Försvarsmaktens handbok för systemsäkerhet*, m7740-784851 edn, Försvarsmakten.

Wiktorin, O. & Ekholm, R. (1996*b*), *System Safety Manual*, m7740-784851 edn, Armed Forces.

Princip-studie av bilbana med avseende på systemsäkerhet

Jonas Biteus, Gunnar Cedersund, Erik Frisk,
Mattias Krysander och Lars Nielsen

E-mail: {biteus, gunnar, frisk, matkr, lars}@isy.liu.se
Department of Electrical Engineering
Linköpings universitet, SE-581 83 Linköping, Sweden

Version 1.1

6 februari 2003

1.1 Sammanfattning

Detta dokument sammanfattar utförandet av säkerhetsanalysen av bilbanan.

Säkerhetsanalysen har genomförts under tiden 020611–030131.

I de efterföljande bilagorna finns: Projektplan; UTTEM; RFP; SSPP; SSWG; SSPR; SRP; PHL; PHA; SRCA; SHA; TES; SRS; FRACAS; SV; SCA / SAR; PHST; SS; TSR; SR; RADS.

Princip-studie av bilbana med avseende på systemsäkerhet

Projektplan

Jonas Biteus

E-mail: biteus@isy.liu.se
Department of Electrical Engineering
Linköpings universitet, SE-581 83 Linköping, Sweden

Version 1.0

3rd February 2003

1.1 Inledning

Projektet kommer genomföras för att skapa djupare kunskap om hur säkerhetsarbete utförs enligt FMVs standard. Genom att förstå hur arbetet utförs ges en bättre koppling meellan det arbete inom FDI sm Fordonssystem utvecklar metoder inom och det säkerhetsarbete som utföres inom SAAB.

1.2 Mål

Analysen syftar till att säkerställa att systemet är säkert. För analysen används försvarets handbok för systemsäkerhet (Wiktorin & Ekholm 1996)

1.3 Aktiviteter

Aktivitet	Ansvarig, resurs	Inst.	Tid.(datum)
TTEM	Lars	HK	020611-0814
RFP	Krysander	FMV	–”–
SSPP	Erik	Ind.	–”–
SSWG	Gunnar	HK, FMV, Ind.	–”–
SSPR	Gunnar	Ind.	–”–
SRP	Jonas	Ind.	–”–
PHL	Krysander, Lars	Ind.	020814-020912
PHA	Erik, Gunnar	Ind.	–”–
SRCA	Jonas	Ind.	–”–
SHA / SSHA	Gunnar, Krysander	FMV, Ind.	020912-021118
O&SHA / EHA	Jonas, Erik	Ind.	020912
TES	Krysander	FMV, Ind.	021118-021216
SRS	Krysander	Ind.	021216-030130
FRACAS	Krysander	HK, FMV, Ind.	–”–
SV	Jonas	Ind.	–”–
SCA / SAR	Krysander	Ind.	–”–
PHST	Jonas	FMV	–”–
SS	Jonas	FMV	030130-030203
TSR	Krysander	HK	–”–
SR	Jonas	HK	–”–
RADS	Krysander	HK, FMV, Ind.	–”–

För mer information se Bild 2.3 i Wiktorin & Ekholm (1996). Vid dessa aktiviteter används FMEA, felträd etc.

1.4 Projektstruktur

- Projektledare: Jonas
- Projektdeltagare: Jonas, Lars, Krysander, Gunnar, Erik
- Start: 020611
- Veckomöten: Nej, månadsmöten efter en inledande period med veckomöten.
- Slut: 030102

1.5 Tidplan

Nedan följer de officiella möten som har hållits. Till dessa kommer ett antal inofficiella möten där arbete har utförts men inga officiella beslut tagits.

020611 Uppstart

020614 Presentation av TTEM, RFP, SSPP, SSWG, SSPR och SRP. Presentationen ska beskriva aktivitetens syfte, genomförande, etc. Presenteras av respektive aktivitetsansvarig.

020624 Resultaten av TTEM, RFP, SSPP, SSWG, SSPR och SRP redovisas. Presenteras av respektive aktivitetsansvarig.

020814 Presentation av SSWG och SSPR. Version 1.0 av TTEM, RFP, SSPP, SRP fastslås. Resultatet av detta ska vara ett kontrakt mellan beställare och en leverantör.

Presentation av PHL, PHA, SRCA av respektive ansvarig.

020823 Utkast till PHL, PHA, SRCA presenteras.

Presentation av SHA / SSHA, O&SHA / EHA och TES av respektive ansvarig. Presentationerna visar på att detta är snarlika problem som genomförs för olika områden. För att kunna analysera problemställningarna beslutas att en fullständig SHA / SSHA genomförs.

020828 En plan för hur en fullständig SHA / SSHA ska genomföras presenteras av Krysander och Gunnar.

020912 Mindre litteraturstudie av de olika delarna inom SHA. Beskrivning av styrsystemet.

SHA / SSHA och O&SHA / EHA är säkerhetsanalyser av olika delar av systemet och med avseende på olika risker. Pga likheterna beslutas att endast en säkerhetsanalys ska genomföras. Styrsystemet, fordon och bana ska granskas med hjälp av FTA och FMEA.

021016 Diskussionsmöte.

021118 FTA och FMEA presenteras och infogas i SHA.

030114 SHA diskussion.

030130 TES, SRS, FRACAS, SV, SCA, SCA, PHST färdigställs

030203 SHA, TES, SRS, FRACAS, SV, SCA, SCA, PHST, SS, TSR, SR och RADS presenteras och fastslås.

I och med SR kan systemet klassas som säkert.

Projektet avslutas.

1.6 Dokument

Till samtliga aktiviteter skrivs ett dokumentavsnitt. Samtliga dokumentavsnitt sammanfattas sedan till ett säkerhetsdokument för bilbanan, bbsp.pdf.

Script för samanställandet av säkerhetsdokumentet finns, ”makedoc.sh”.

References

Wiktorin, O. & Ekholm, R. (1996), *Försvarsmaktens handbok för systemsäkerhet*, m7740-784851 edn, Försvarsmakten.

This page intentionally left empty.

UTTEM
Utkast till Taktisk Teknisk Ekonomisk Målsättning

NFFP

Redaktör: Lars Nielsen
Version: 1.1

Status

Granskad	Nielsen	020617
Godkänd	Nielsen	020912

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2002
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
0.1	020617	Första utkastet.	Lars
1.1	020912	Version 1.1.	Lars

Innehåll

1 UTTEM

Detta UTTEM (Utkast till Taktisk Teknisk Ekonomisk Målsättning) avser säkerheten för projektet Bilbanestyrning. Bakgrundsinformation finns i projektbeskrivningen av detta projekt.

Övergripande säkerhetskrav är

Krav	Version	Beskrivning	Prioritet
1		Vid körning tolereras maximalt 1 avåkning per 100 körda varv. Med avåkning menas att bilen inte kan fortsätta körningen utan manuella ingrepp.	1
2		Bilarna får inte köras så snabbt att de riskerar att lämna banan och orsaka person- eller större materialskada. Detta gäller även under utvecklingen.	1
3		Programmet får inte innehålla konstruktioner som låser Matlabs kommandotolk mer än 0.05 sekund. Kravet finns av säkerhetsskäl, för att undvika att bilarna kör av banan. Kravet verifieras med tic-toc i Matlab.	1

Vad gäller säkerheten delas banan in i tre olika typer av segment: α, β, γ. För α-segment gäller höga säkerhetskrav och höga prestandakrav. Det är segment av banan där en avåkning är katastrofal, men där det samtidigt är viktigt med hög fart och höga krav på exakthet i hastighet och timing (pga samverkan med andra system (t.ex. leverans av last)). För β-segment gäller höga säkerhetskrav men kraven på prestanda är inte kritiska. En avåkning är katastrofal men man kan alltså köra en aning försiktigare här. För γ-segment är en avåkning inte katastrofal (man är kvar på bordet).

RFP
Kravställning vid offertförfrågan
NFFP

Redaktör: Mattias Krysander
Version: 1.0

Status

Granskad	Krysander	020814
Godkänd	Nielsen	020814

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2002
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
0.1	020617	Första utkastet.	Gunnar
0.9	020814	Förslag av slutlig RFP	Gunnar
1.0	020814	Slutlig RFP	Gunnar

Innehåll

1 RFP

Detta RFP (Kravställning vid offertförfrågan) avser säkerheten för projektet Bilbanestyrning. Bakgrundsinformation finns i projektbeskrivningen av detta projekt.

Övergripande säkerhetskrav är

1.1 Krav på aktiviteter för systemsäkerhetsverksamheten

Kraven har klassificerats som skall-krav (utmärkta med prioritet 1) och bör-krav (utmärkta med prioritet 2). De krav som saknar prioritet kan i nuläget ej klassificeras. Samtliga krav utförs enligt beskrivning i H SystSäk.

Krav	Version	Beskrivning	Prioritet
1		Säkerhetskrav i TTEM upprättas.	1
2		Säkerhetskrav i RFP upprättas.	1
3		SSPP upprättas.	1
4		SSWG inrättas.	
5		SSRP sker.	
6		SRP upprättas.	
7		PHL upprättas.	
8		PHA upprättas.	
9		SRCA genomföras.	
10		SHA/SSHA genomföras.	
11		O&SHA genomföras.	
12		TES genomföras.	
13		SRS uformas.	
14		FRACAS upprättas.	
15		SV upprättas.	
16		SCA med SAR upprättas.	
17		PHST bör upprättas.	2
18		SS skall upprättas.	1
19		TSR bör upprättas.	2
20		SR skall upprättas.	1
21		RADS bör genomföras.	2

1.2 Materielkrav

1.2.1 Operativt inriktade krav

Krav	Version	Beskrivning	Prioritet
22		Vid körning tolereras maximalt 1 avåkning per 100 körda varv. Med avåkning menas att bilen inte kan fortsätta körningen utan manuella ingrepp.	1
23		Bilarna får inte köras så snabbt att de riskerar att lämna banan och orsaka person- eller större materialskada. Detta gäller även under utvecklingen.	1
24		Största acceptabla säkerhetsavståndet för användning av systemet är bordskanten.	1
25		Vad gäller säkerheten delas banan in i tre olika typer av segment: α, β, γ. α-segmentet är den del av banan som är närmst dörren och begränsas av vita markeringar på banan .För α-segment gäller höga säkerhetskrav och höga prestandakrav. Det är segment av banan där en avåkning är katastrofal, men där det samtidigt är viktigt med hög fart. α-segmentet ska avklaras på maximalt 0.1 sekunder längre tid än den kortaste tiden utan avåkning. Detta tidskrav ska vara uppfyllt förutsatt att kollisionsrisk ej förestår.	1
26		Felet på skattningen av hastigheten får som mest vara 3 % under hela α-segmentet.	1
27		Säkerhetsavståndet mellan två bilar vid ingång till och genom avsmalning är en halv billängd.	1
28		β-segment är de partier av banan som ej är ingår i α-segmentet och där avåkning med resulterar i avåkning från bordet. Detta definieras som de punkter på banan där bordkanten befinner sig mindre än 50 cm från positionen i rörelseriktningen. För β-segment gäller att vid körning tolereras maximalt 1 avåkning per 1000 varv.	1
29		I kurvor på β-segment ska hastigheten inte understiga 80% av den hastigheten som får bilarna till en lätt avåkning. På β-segmentens raka partier gäller att den minimala hastigheten är den samma som i framförvarande kurva.	1
30		Före varje körning ska säkerhetskontrollen utföras på högst en minut.	1

1.2.2 Konstruktionskrav

Krav	Version	Beskrivning	Prioritet
31		Uppsättning av oelastiska barriärer är ej tillåtet.	1
32		Sensorer på banan får inte kunna orsaka personskador.	1
33		Aktuatorer längs banan får inte kunna orsaka personskador.	1
34		Programmet får inte innehålla konstruktioner som låser Matlabs kommandotolk mer än 0.05 sekund. Kravet finns av säkerhetsskäl, för att undvika att bilarna kör av banan. Kravet verifieras med tic-toc i Matlab.	1

Systemsäkerhetsplan (SSPP)

NFFP

Redaktör: Erik Frisk
Version: 1.0

Status

Granskad	Erik Frisk	2002-08-14
Godkänd	Jonas Biteus	020912

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2002
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
0.1	020623	Första utkastet.	Erik
1.0	020814	Slutversion	Erik

Innehåll

1 Beskrivning av systemet

1.1 Teknisk och operativ beskrivning

En teknisk och operativ beskrivning av hur systemet är tänkt att fungera finns i kravspecifikationen.

1.2 Gällande systemsäkerhetskrav

Gällande systemsäkerhetskrav finns beskrivna i SRP och riskvärderingen ska ske enligt avsnitt 1.12.1 i [1].

2 Organisation och ansvar

Varje konstruktör ser till, efter bästa förmåga, att säkerhetskraven uppfylls för den del av systemet som konstruktören själv ansvarar för. Säkerhetsarbetet granskas sedan av en, på förhand utsedd, grupp kollegor.

Ansvar för säkerhetskraven har industringruppens säkerhetsavdelning.

3 Säkerhetsaktiviteter

Följande säkerhetsaktiviteter ska genomföras under projektutvecklingen (baserat på RFP samt [1].

Krav	Version	Beskrivning	Prioritet
1		Säkerhetskrav i TTEM upprättas.	1
2		Säkerhetskrav i RFP upprättas.	1
3		SSPP upprättas.	1
4		SSWG inrättas.	
5		SSRP sker.	
6		SRP upprättas.	
7		PHL upprättas.	
8		PHA upprättas.	
9		SRCA genomföras.	
10		SHA/SSHA genomföras.	
11		O&SHA genomföras.	
12		TES genomföras.	
13		SRS uformas.	
14		FRACAS upprättas.	
15		SV upprättas.	
16		SCA med SAR upprättas.	
17		PHST bör upprättas.	2
18		SS skall upprättas.	1
19		TSR bör upprättas.	2
20		SR skall upprättas.	1
21		RADS bör genomföras.	2

Tidplanering av ovanstående uppgifter sker enligt [1].

4 Dokumentation, referenser, tillämpliga standarder

Nedanstående dokument är alla nödvändiga för att säkerhetsarbetet ska kunna följas. Alla dokument ska finnas tillgängliga i projektbiblioteket.

Dokument	Fastställare
SSPP	Erik
SCA/SAR	Enligt BBSP-projektplan
SSPR	Enligt BBSP-projektplan
FRACAS	Enligt BBSP-projektplan

Referenser

[1] Försvarsmakten. *Försvarsmaktens handbok för Systemsäkerhet - H SystSäk*. FM, 1996.

SSWG
System Safety Working Group
NFFP

Redaktör: Gunnar Cedersund
Version: 0.2

Status

Granskad	Gunnar Cedersund	020902
Godkänd		

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2002
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
0.1	020814	Första utkastet.	Gunnar
0.2	020902	Olyckstillbud rapporterat.	Jonas

Innehåll

1 Allmän information

System Safety Working Group (SSWG) är den verkställande delen av systemet och består av en grupp människor vars antal kan variera under de olika delarna av processen. Det är SSWG som skriver de olika rapporterna som utgör System Safety Progress Reviews (SSPR) och som är specificerade i System Safety Program Plan (SSPP). SSWG finns med hela tiden från dess skapande under planeringsfasen till och med användandet och återvinningen av färdig produkt och beroende på projektets omfattning och aktuell fas kan SSWG variera i storlek samt delas in i olika subgrupper. Till sin hjälp har de möjlighet att konsultera experter från t ex industrin.

2 Personer

2.1 I SSWG

De personer som utgör SSWG, och alla dess undergrupper i detta projekt är:
Gunnar Cedersund
Lars Nielsen
Mattias Krysander
Erik Frisk
Jonas Biteus (projektledare)

2.2 Experter

Expert från industrin i detta projekt är Per Andersson och Per Öberg.

3 Incident list

Detta avsnitt inkluderar en lista över alla incidenter som har inträffat under utveckling, användning och “disposal”.

3.0.1 Bilkrash

Fas: Utveckling

Skada: En förstörd bil.

Risk för skada: Förstörd fönsterruta. En förstörd fönsterruta skulle ha kunnat orsaka personskada genom skärsår. Om en person stått utanför fönstret skulle an allvarlig skada kunnat inträffa.

Orsak: Då pådrag skulle ges till styrsystemet användes felaktigt kommandot `<set-manual-speed(0.2)>` istället för det korrekta `<set-car-speed(0.2)>`. Kommandot skulle ge 20% pådrag.

Resultat: Styrsystemet gav bilen maximalt med pådrag vilket resulterade i att bilen med hög fart körde av banan. Räcken deflekterade bilen uppåt och vid landning på golv skadades bilen.

Förslag till åtgärd: Endast funktioner som är korrekta finns i katalogen och sökvägen.

Rapportör: Jonas

Åtgärd beslutad av SSWG:

SSPR
System Safety Progress Reviews
NFFP

Redaktör: Gunnar Cedersund
Version: 0.1

Status

Granskad	Gunnar	020814
Godkänd	Gunnar	020814

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2002
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
0.1	020814	Första utkastet.	Gunnar

Innehåll

1 Allmän information

System Safety Progress Reviews (SSPR) är samlingsnamnet för alla interna rapporter inom System Safety Working Group (SSWG), samt för alla status-rapporter till Försvarets Materialverk (FMV) och Armed Forces' Medical Center (FSC). SSPR innehåller därför alla rapporter som är specificerade i den preliminära systemsäkerhetsplanen (SSPP). Rapporterna ligger till grund för diskussioner och slutligen för beslut angående den fortsatta verskamheten.

2 Uppdrag från SSPP

Följande säkerhetsaktiviteter ska enligt SSPP genomföras under projektutvecklingen:

Krav	Version	Beskrivning	Prioritet
1		Säkerhetskrav i TTEM upprättas.	1
2		Säkerhetskrav i RFP upprättas.	1
3		SSPP upprättas.	1
4		SSWG inrättas.	
5		SSRP sker.	
6		SRP upprättas.	
7		PHL upprättas.	
8		PHA upprättas.	
9		PHL genomföras.	
10		SRCA genomföras.	
11		SHA/SSHA genomföras.	
12		O&SHA genomföras.	
13		TES genomföras.	
14		SRS uformas.	
15		FRACAS upprättas.	
16		SV upprättas.	
17		SCA med SAR upprättas.	
18		PHST bör upprättas.	2
19		SS skall upprättas.	1
20		TSR bör upprättas.	2
21		SR skall upprättas.	1
22		RADS bör genomföras.	2

SRP
Säkerhetsdel i Offert för Bilbanestyrning

NFFP

Redaktör: Jonas Biteus
Version: 1.0

Status

Granskad	Biteus	020623
Godkänd	Biteus/Nielsen	020813

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2002
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
0.1	020623	Första utkastet.	Biteus
0.9	020813	Förslag från leverantör.	Biteus
1.0	020815	Kontrakt HQ/industri.	Biteus

Innehåll

1 SRP

Denna SRP beskriver säkerhetsdelen i offert för projekt bilbanestyrning. RFP (Kravställning vid offertförfrågan) har ställts av Mattias Krysander.

I dokumentet beskrivs dom säkerhetskrav som offertställaren anser nödvändiga. De följer delvis RFP, skillnader markeras med *.

1.1 Krav på aktiviteter för systemsäkerhetsverksamheten

Kraven har klassificerats som skall-krav (utmärkta med prioritet 1) och bör-krav (utmärkta med prioritet 2). De krav som saknar prioritet kan i nuläget ej klassificeras. Samtliga krav utförs enligt beskrivning i H SystSäk.

Krav	Version	Beskrivning	Prioritet
1		Säkerhetskrav i TTEM upprättas.	1
2		Säkerhetskrav i RFP upprättas.	1
3		SSPP upprättas.	1
4		SSWG inrättas.	
5		SSRP sker.	
6		SRP upprättas.	
7		PHL upprättas.	
8		PHA upprättas.	
9		PHL genomföras.	
10		SRCA genomföras.	
11		SHA/SSHA genomföras.	
12		O&SHA genomföras.	
13		TES genomföras.	
14		SRS uformas.	
15		FRACAS upprättas.	
16		SV upprättas.	
17		SCA med SAR upprättas.	
18		PHST bör upprättas.	2
19		SS skall upprättas.	1
20		TSR bör upprättas.	2
21		SR skall upprättas.	1
22		RADS bör genomföras.	2

1.2 Materielkrav

Krav	Version	Beskrivning	Prioritet
23		Självsläckande material ska användas i bana (med kringutrustning, t.ex. räcken) samt i bilar.	1*
24		Strömförsörjningen till bilbanan ska vara utrustad med säkringar.	1*

1.2.1 Operativt inriktade krav

Krav	Version	Beskrivning	Prioritet
25		Vid körning tolereras maximalt 1 avåkning per 100 körda varv. Med avåkning menas att bilen inte kan fortsätta körningen utan manuella ingrepp.	1*
26		Bilarna får endast köras i en riktning. Denna markeras med röd pil på banan vid fyra ställen.	1*
27		Om bilar körs åt fel håll ska styrsystemet avbryta körningen senast när en bil passerat två sensorer.	1*
28		Vid körning tolereras maximalt 1 allvarlig avåkning per 400 körda varv. Med allvarlig avåkning menas att bilen fullständigt lämnat banan eller att bilen har hamnat upp och ner.	1*
29		Bilarna får inte köras så snabbt att de riskerar att lämna banan och orsaka person- eller större materialskada. Detta gäller även under utvecklingen.	1
30		Säkerhetsavståndet för användning av systemet är bordskanten eller 0.4 m från bilbanan där bordskanten befinner sig mer än 0.4 m från bilbanan. Med användning menas att bilarna rör sig eller att spänningen till bilbanan inte är noll.	1*

Vad gäller säkerheten delas banan in i tre olika typer av segment: α, β, γ. α-segmentet är den del av banan som är närmst dörren samt den del som är närmast datorn. Dessa segment begränsas av vita markeringar på banan. För α-segment gäller höga säkerhetskrav och höga prestandakrav. Det är segment av banan där en avåkning är katastrofal, men där det samtidigt är viktigt med hög fart.

Krav	Version	Beskrivning	Prioritet
31		α-segmentet ska avklaras på maximalt $5\,s$ sekunder förutsatt att kollisionsrisk eller avåkningsrisk ej förestår.	1
32		Felet på skattningen av hastigheten får som mest vara 3 % under hela α-segmentet.	1
33		Maximalt en (1) bil får vara i avsmalningssegmentet av banan vid någon tidpunkt. Avsmalningssegmentet definieras som den del där avsmalningen i banan finns, samt sträckorna fram till närmaste sensordel (framåt och bakåt). Om två bilar befinner sig inom området ska den bil som senast inträdde i området stannas tills dess att maximalt en bil är kvar inom segmentet.	1*

fortsättning nästa sida

fortsättning från föregående sida			
Krav	Version	Beskrivning	Prioritet
34		β-segment är de partier av banan som ej ingår i α-segmentet och där avåkning resulterar i avåkning från bordet. Detta definieras som de punkter på banan där bordkanten befinner sig mindre än 20 cm från positionen i rörelseriktningen. För β-segment gäller att vid körning tolereras maximalt 1 avåkning per 1000 varv.	1
35	Ej säkerhets-kritiskt.	I kurvor på β-segment ska hastigheten inte understiga 80% av den hastigheten som får bilarna till en lätt avåkning. Med lätt avåkning menas att bilen befinner sig rättvänd (m.a.p. rörelseriktning) och inte har snurrat (t.ex. upp och ner), samt befinner sig på banan. På β-segmentens raka partier gäller att den minimala hastigheten är den samma som i framförvarande kurva.	5*

1.2.2 Konstruktionskrav

Krav	Version	Beskrivning	Prioritet
36		Barriärer ska vara elastiska.	1*
37		Barriärer ska finnas vid kurvor samt 20 cm efter varje kurvas slut i körriktningen.	1*
38		Barriärer ska vara 2.5 cm höga i lätta kurvor vilket defineras som den minsta kurvvarianten som finns på banan. Övriga barriärer ska vara 5 cm höga.	1*
39		Sensorer på banan får inte kunna orsaka personskador.	1
40		Aktuatorer längs banan får inte kunna orsaka personskador.	1
41		Programmet får inte innehålla konstruktioner som låser Matlabs kommandotolk mer än 0.05 sekund. Kravet finns av säkerhetsskäl, för att undvika att bilarna kör av banan. Kravet verifieras med tic-toc i Matlab.	1
42		Samtlig mjukvara ska kontrolleras av annan person är programmeraren innan den får användas.	1*
43		Samtliga kommandon i mjukvara, med undantag för triviala, ska dokumenteras.	1*
44		Varje rad i mjukvaran får utföra maximalt en (1) funktion.	1*

PHL
Preliminär riskkälleanalys
NFFP

Redaktör: Mattias Krysander & Lars Nielsen
Version: 1.0

Status

Granskad	Krysander,Nielsen	020815
Godkänd	Krysander,Nielsen	020815

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2002
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
1.0	020815	Slutlig PHL	

Innehåll

1 Preliminär riskkälleanalys (PHL)

Lista på tänkbara riskkällor inom projektet för Bilbanestyrning som kan orsaka skada på person, egendom eller yttre miljö.

1.1 Energirelaterade riskkällor

Explosiva föremål

Riskkälla	Beskrivning	Kommentarer
1	Elektrolytkondensatorer på sensorportalelektronik	

Explosiv atmosfär

Roterande maskindelar

Riskkälla	Beskrivning	Kommentarer
2	Bilhjul	

Utkastade maskindelar

Riskkälla	Beskrivning	Kommentarer
3	Bilar	urspårad bil

Varma delar

Riskkälla	Beskrivning	Kommentarer
4	Transformator	

Spända fjädrar

Riskkälla	Beskrivning	Kommentarer
5	Fjädrar i reglage	

Tryckkärl, system under tryck

Ljudtryck

Strömförande delar

Riskkälla	Beskrivning	Kommentarer
6	Skenor i körbanan	
7	Transformator	
8	Styrburk	
9	Styrkort	
10	Anslutningssladdar mellan uttag och skenor via dator	
11	Anslutningssladdar mellan uttag och styrburk via transformatorn	
12	Sensorer	
13	Sensorportalelektronik	
14	Sensorburk	
15	Sensorkort	
16	Anslutningssladdar mellan dator och sensorer	

Elektromagnetisk strålning

Riskkälla	Beskrivning	Kommentarer
17	Datorskärm	

Laddade kondensatorer

Riskkälla	Beskrivning	Kommentarer
18	Elektorlytkondensatorer på sensorportalelektronik	

Elektrostatisk energi

Ackumulatorer

Fallande föremål, rörliga föremål, t ex dörrar

Laser

UV-ljus

Riskkälla	Beskrivning	Kommentarer
19	Optiska sensorer	Per Öberg anser inte att det föreligger någon risk.

1.2 Vassa kanter

Riskkälla	Beskrivning	Kommentarer
20	Lödningar av sensorportaler	

1.3 Riskfyllda substanser

Brandfarliga ämnen

Riskkälla	Beskrivning	Kommentarer
21	T-röd för rengöring av körbanor	
22	Trasor för rengöring av körbanor	
23	Stolar	
24	Bord	

Självantändande ämnen

Gasutvecklande ämnen

Riskkälla	Beskrivning	Kommentarer
25	PVC i sladdar	

Oxiderande ämnen

Frätande ämnen

Giftiga ämnen

Radioaktiva ämnen

1.4 Övriga risker

Höjdskillnad

Riskkälla	Beskrivning	Kommentarer
26	Bord	För att nå vissa delar av banan krävs det att användare går upp på bordet.

Hala ytor

Tryckskillnader

Syrebrist

Kvävning

Kyla

Värme

Ergonomiskt ensidig belastning

Riskkälla	Beskrivning	Kommentarer
27	Reglage	

Vibrationer

Buller

Bländning

PHA
Preliminär riskanalys
NFFP

Redaktör: Erik Frisk & Gunnar Cedersund
Version: 1.0

Status

Granskad	Frisk, Cedersund	020822
Godkänd	Frisk Cedersund	020822

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2002
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
1.0	020822	Slutlig PHA	

Innehåll

1 Preliminär riskanalys (PHA)

Preliminär riskkälleanalys är ett grovt verktyg för att identifiera och dokumentera risker med tillhörande vådahändelser.

Allvarlighetsgrad	Betydelse
I	Död, systemförlust eller allvarlig miljöskada
II	Allvarlig peronsskada, allvarlig egendomsskada
III	Mindre allvarlig personskada, mindre skada på egendom eller mindre miljöskada
IV	Mindre omfattning än ovan

1	Elektrolytkondensator på sensorportalelektronik exploderar	
	Konsekvens	Ansikts, ögon, eller skador på händer,
	Allvarlighetsgrad	III
	Orsaker	Felkopplad matning till elektronik För hög ström genom kondensator
	Skyddsåtgärd	Väldimensionerad skyddsdiod
2	Bilhjulet roterar	
	Konsekvens	Bilen kör framåt
	Allvarlighetsgrad	0
	Orsaker	Att man gasar
	Skyddsåtgärd	sluta gasa
3	Bilen kastas ut från körbanan	
	Konsekvens	Uppdraget misslyckas eller blir försenat. Ev allvarlig personskada och tom död (av virtuella föraren)
	Allvarlighetsgrad	I
	Orsaker	För hög hastighet in i kurva. Ojämnhet i banan, t ex litet mellanrum mellan delar.
	Skyddsåtgärd	Sätt upp sidoräcken. Sänk hastigheten. Dessa åtgärder speciellt på kritiska ställen. Där bör också testkörningen vara mer noggran. Eventuellt kan vägen också lutas lite mot kurvan.
4	Transformatorn blir för varm	
	Konsekvens	Någon bränner sig. Eventuell brand.
	Allvarlighetsgrad	II
	Orsaker	Transformatorn glöms på. Någonting flamfarligt läggs emot. Eventuella inre orsaker.
	Skyddsåtgärd	Sätt en timer eller termostat på. Varna när temperaturen är för hög. Skaffa bra rutiner för avstängning.
5	Fjädrar i reglage lossnar och hoppar iväg	
	Konsekvens	Förlorad fjädereffekt. Eventuellt kan fjäder 'hoppa på' någon

	Allvarlighetsgrad	IV
	Orsaker	Fjädern felaktigt ditsatt.
	Skyddsåtgärd	Kontrollera ditsättningen
6	Skenor i körbanan strömförande/ingen strömförsörjning	
	Konsekvens	Ström genom operatör, eller stillastående bil
	Allvarlighetsgrad	III
	Orsaker	Otrolig kortslutning
	Skyddsåtgärd	Är redan åtgärdat enligt Lars.
7	Tranformator kortlusten eller strömförande	
	Konsekvens	Ström genom operatör eller stillastående bil.
	Allvarlighetsgrad	III
	Orsaker	Överladdning eller utslitning eller inre fel
	Skyddsåtgärd	Använd utrustningen med sunt förnuft
8	Styrburk strömförande	
	Konsekvens	Operören får en stöt
	Allvarlighetsgrad	IV
	Orsaker	Inre elektriskt problem hos styrburk
	Skyddsåtgärd	använd skyddshandskar
9	Styrkort kortsluten	
	Konsekvens	Utrustningen funkar inte
	Allvarlighetsgrad	III
	Orsaker	Kortslutning
	Skyddsåtgärd	Byt ut kortet. Kolla det innan programmet startas
10	Sladdar mellan uttag och skenor glapp, kortslutna, strömförande eller stulna	
	Konsekvens	Strömmen går inte fram eller ut till operör
	Allvarlighetsgrad	III
	Orsaker	se namn
	Skyddsåtgärd	kontrollera sladdar och vid behov byt ut dem mot nyköpta
11	Sladdar mellan uttag och styrburk glapp, kortslutna, strömförande eller lånade	
	Konsekvens	Strömmen går inte fram (systemet ur funktion) eller in i den stackars operatören
	Allvarlighetsgrad	III
	Orsaker	Utslitna sladdar (eller lånade)
	Skyddsåtgärd	Kontrollera och byt ut sladdar. (eller låna tillbaka dem)
12	Sensorer kortslutna	
	Konsekvens	Felaktig sensorsignaler ger felaktiga beslut eller verkställanden
	Allvarlighetsgrad	III
	Orsaker	sensorer kortslutna
	Skyddsåtgärd	byt mot nya
13	Sensorportalelektronik ur funktion	
	Konsekvens	Felaktig sensorsignaler ger felaktiga beslut eller verkställanden

	Allvarlighetsgrad	II
	Orsaker	Utrustning utsliten
	Skyddsåtgärd	Köp ny
14	Sensorburk strömförande	
	Konsekvens	ström genomströmmande operatör
	Allvarlighetsgrad	III
	Orsaker	Kortslutning ledande ström till burk
	Skyddsåtgärd	köp dubbla burkar
15	Sensorkort strömförande	
	Konsekvens	Ström genom kroppen hos operatör
	Allvarlighetsgrad	III
	Orsaker	Kortslutning
	Skyddsåtgärd	Se till att sensorkort är väl inkapslade och ej blottlagda
16	Anslutningssladdar mellan dator och sensorer strömförande	
	Konsekvens	Ström genom kroppen hos operatör
	Allvarlighetsgrad	IV
	Orsaker	Sönderskavda sladdar
	Skyddsåtgärd	Se till att sladdar är väl inbundna och fastgjorda vid bordet
17	Elektromagnetisk strålning från datorskärm	
	Konsekvens	Böld på nästippen
	Allvarlighetsgrad	IV
	Orsaker	Den fungerar så
	Skyddsåtgärd	Byt till TFT-skärm
18	Elektrolytkondensatorer på sensorportalelektronik laddade	
	Konsekvens	minimal
	Allvarlighetsgrad	
	Orsaker	
	Skyddsåtgärd	
19	UV-ljus från optiska sensorer	
	Konsekvens	Ögonskada
	Allvarlighetsgrad	IV
	Orsaker	
	Skyddsåtgärd	
20	Vassa kanter hos lödningarna av sensorportaler	
	Konsekvens	Skrapsår på fingrar
	Allvarlighetsgrad	IV
	Orsaker	Lödning ger vassa kanter
	Skyddsåtgärd	Köp plåster
21	T-röd för rengöring av körbanor brandfarligt	
	Konsekvens	Brandskada hos operatör
	Allvarlighetsgrad	II
	Orsaker	Rökare i lokalen

		Barn och tändare i lokalen
	Skyddsåtgärd	
22	Trasor för rengöring av körbanor brandfarliga	
	Konsekvens	Brandskada hos operatör
	Allvarlighetsgrad	II
	Orsaker	Rökare i lokalen Barn och tändare i lokalen
	Skyddsåtgärd	
23	Brandfarliga stolar	
	Konsekvens	Brandskada hos operatör
	Allvarlighetsgrad	II
	Orsaker	Rökare i lokalen Barn och tändare i lokalen
	Skyddsåtgärd	
24	Brandfarliga bord	
	Konsekvens	Eventuell brand
	Allvarlighetsgrad	II
	Orsaker	brandfarliga bord
	Skyddsåtgärd	
25	Gasutveckling från PVC i sladdar	
	Konsekvens	Illamående hos operatör
	Allvarlighetsgrad	III
	Orsaker	cirkulerande bil
	Skyddsåtgärd	
26	Fall från bord	
	Konsekvens	Kroppsskada
	Allvarlighetsgrad	III
	Orsaker	
	Skyddsåtgärd	
27	Ergonomisk belastning från användning av reglage	
	Konsekvens	Värk i hand
	Allvarlighetsgrad	IV
	Orsaker	Monoton belastning av hand
	Skyddsåtgärd	Gå på både 10 och 3-fikat

SRCA
Analys av säkerhetskrav och säkerhetskriterium
NFFP

Redaktör: Jonas Biteus
Version: 1.0

Status

Granskad	Jonas Biteus	030131
Godkänd	Mattias Krysander	030131

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2003
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
1.0	030131	Version ett	Jonas

Innehåll

1 Inledning

Syftet med SRCA (analys av säkerhetskrav och säkerhetskriterium) är att identifiera säkerhetskrav som är relevanta för systemet. Till grund för detta ligger PHL (preliminär risklista) och PHA (preliminär riskanalys). Kraven kan vara tekniska, lagtekniska mm.

Sysfemsäkerhet och designkrav för både hårdvara och mjukvara ska bestämmas och definieras i både system- och designkraven. See SRP (säkerhetsdel i offert).

Det skall vara möjligt att verifiera all säkerhetsrelaterade krav, see SV (säkerhetsverifikation).

2 Analys av säkerhetskrav och säkerhetskriterium

De krav som ställs på systemet framgår av SRP. Det vill säga SRP:s kravlista accepteras utan förändringar som de krav som ska ställas på systemet.

SHA
Säkerhetsanalys för system
NFFP

Redaktör: Mattias Krysander
Version: 1.1

Status

Granskad	Mattias Krysander	021115
Godkänd	Jonas Biteus	021118

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2002
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
0.1	020827	Disposition	
1.0	021118	Slutlig SHA	Krysander, Biteus
1.1	030130	Mindre förändringar, Biteus	

Innehåll

1 Allmänt om SHA

Säkerhetsanalys för system (SHA), är en fortsatt och fördjupad analys av säkerheten för systemet i fråga som är påbörjad i och med PHL och PHA.

Förslag på arbetsgång:
Analysera vådahändelser angivna i PHL och PHA med felträdsanalys (FTA). FTA:n genererar bland annat bashändelser. Dessa bashändelser plus eventuellt ytterligare upptäckta bashändelser analyseras i feleffektanalys (FMEA). FMEA:n identifierar enkelfel som kan leda till vådahändelser och fel med gemensam orsak. Båda av dessa två typer av fel bör elimineras. Därför upprättas en åtgärdslista där dessa fel samt korrigerande åtgärd noteras. I analyserna av hård- och programvara ska bidragen till systemsäkerheten bestämmas. Kontrollera att införande av nya krav eller åtgärder inte minskar systemsäkerheten. Slutligen kontrolleras att de konstruktiva säkerhetskriterierna är uppfyllda.

Sammanfattning:

1. Analysera vådahändelser i PHA med FTA.
2. Analysera de i FTA hittade bashändelser med FMEA. Undersök nyupptäckta vådahändelser i punkt (1).
3. Upprätta en lista med enkelfel och fel med gemensam orsak. Felen listas som i en FMEA plus att förslag på åtgärder för att eliminera eller i andra hand minska konsekvens och eller sannolikhet för felet bifogas.
4. SSWG beslutar vilka åtgärder som ska genomföras. Åtgärderna analyseras från punkt (1). På så sätt säkerställs att åtgärderna ökar systemsäkerheten.
5. Kontrollera att de konstruktiva säkerhetskriterierna är uppfyllda.

2 Arbetsområden inom bilbane projektet

Här följer en uppdelning, och detaljerad beskrivning, av de olika områden som säkerhetsanalysen av bilbanan bör omfatta. Under rubriken finns just nu bara ett namn. Detta är den som är tänkt ska arbeta som huvudansvarig med området.

2.1 Fel på bilbanan

Gunnar ansvarig

2.2 Fel på styrsystem

Jonas ansvarig

2.3 Fel på säkerhetsanordningar/skyddsutrustning

Lars ansvarig

2.4 Inverkan av kringsystem såsom underhållsverktyg

Lars ansvarig

2.5 Inverkan av felaktigt beteende hos operatör

Mattias ansvarig

3 Arbetsplan

Här följer en lite mer detaljerad arbetsplan av hur del olika momenten i SHAn ska inläras och utföras:

1. Inläsning av var sin metod (FTA(Mattias), FMEA(Gunnar), Logiska metoder(Jonas)).
2. Presentation av och diskussion runt metoderna
3. Alla börjar på sin tilldelade uppgift och applicerar lämpliga metoder på denna
4. SSWG möte
5. Iterera

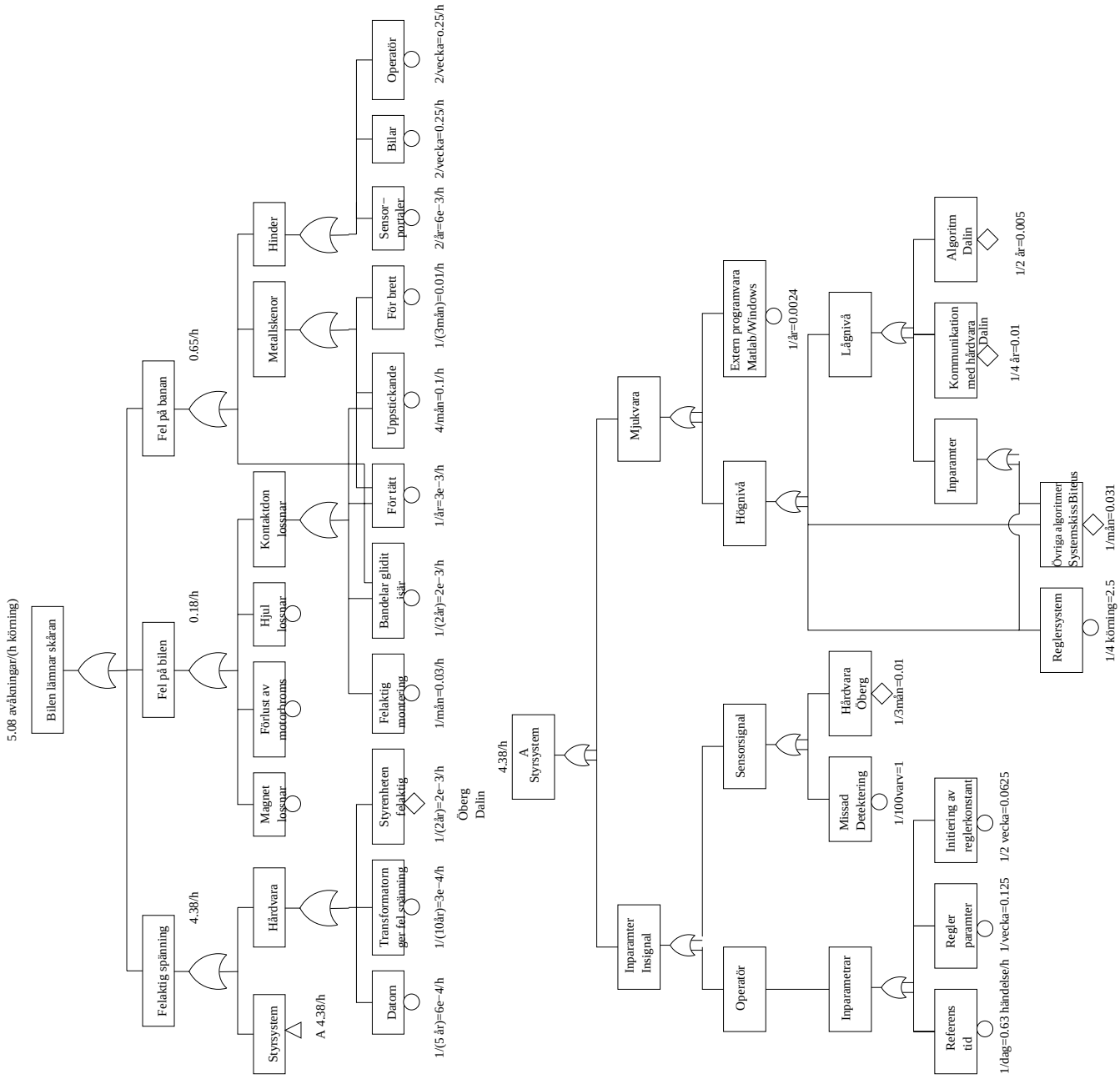
4 Feleffektanalys (FMEA)

Del	Mod	Orsak	Feleffekt	Frekvens	Konsekvens	RPN
Fordon	Hjul lossnar	Slitage	Avkörning, flygande delar	C	II	9
	Kontaktdon	Felaktig montering	Ingen kraft	E	III	15
		Slitage	Avkörning	D	II	8
Styrsystem,	Operatör ger	Referens	Felkontroll avvärjer	B	IV	8
Indata	fel indata	Reglerparameter	Avkörning	B	I	2
		Reglerinitiering	Avkörning	B	I	2
	Sensorsignal	Missad detektion	Avkörning	D	II	8
		Hårdvara	Avkörning	E	II	10
Styrsystem,	Högnivå	Reglersystemet	Avkörning	A	II	2
mjukvara		Kommunikation	Avkörning	E	II	10
	Lågnivå	Styrfunktioner, hårdvara	Avkörning	D	I	4
Styrsystem,	Dator	Strömförsörjning	Elektrisk skada	E	I	5
Hårdvara	Kopplingsdosa	Strömförsörjning	Elektrisk skada	D	I	4
		Elektronik	Avkörning	E	I	5
Bana	Metallskenor	För tätt	Fordonet fastnar	D	II	8
		För brett	Ingen kraft	C	III	9
		Uppstickande	Avkörning	A	II	4
	Hinder	Sensorportal	Avkörning	B	II	4
		Fordon	Avkörning	B	II	4
		Operatör	Avkörning, direkt skada	C	I	3

Notera: Då avkörningar kan föregås av en mycket hög hastighet klassas som risk *I*. Detta kan till exempel förekomma om styrfunktionerna till hårdvaran fallerar och ger 100% pådrag. Med 100% pådrag uppnår fordonet en mycket hög hastighet (10-30 km/h). En avkörning vid denna hastighet kan orsaka direkt eller indirekt personskada. Den allvarligaste indirekta skadan kan uppkomma då fordonet träffar glasrutan som spricker och faller ner, vilket kan orsaka en allvarlig direkt personskada.

Övriga avkörningar klassas som risk *II*. Till exempel då fordonet rullar av i en kurva pga lite för hög hastighet. Detta uppkommer till exempel då referenstiden ligger nära den minimala tiden.

5 Felträdsanalys (FTA)



Styrsystem: Delvis dåligt implementerade algoritmer. Stabilitet ej visad. Har inga begränsningar i pådrag.

Missad detektering: Missad detektering leder till felaktigt pådrag från styrsystemet. T.ex. en skarp kurva när styrsystemet tror vi är på en raksträcka.

Notera: Den totala frekvensen av avkörningar är *5.08 avkörningar per timme*. Den största bidragsfaktorn är styrsystemet med *4.38 avkörningar per timme*. Utav dess 4.38 kommer majoriteten från reglersystemet med *2.5*, missad detektering *1.0* och felaktig referenstid från operatören med *0.63 händelser per timme*.

TES Provningsvärdighet

NFFP

Redaktör: Mattias Krysander
Version: 1.0

Status

Granskad	Krysander	021210
Godkänd	Krysander	021216

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2003
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
1.0	021210	Slutlig TES	Krysander

Innehåll

1 Provningsvärdighet (TES)

Provningsvärdighet (TES) anger de aktiviteter som erfodras för att systemet skall få provas i de fall där risk för skada på person, egendom eller yttre miljö föreligger. TES sker innan provtillfälle.

För att provkörning av bilbanan ska tillåtas måste banans trafikvärdighet godkännas.

1.1 Hanteringsgodkännande

Hanteringsgodkännande säkerställer att övervägande om materielens personsäkerhet har gjorts samt att de eventuella restriktioner, som åläggas användningen, är framtagna och meddelade användaren.

1.1.1 Kontroll av banan

Krav	Version	Beskrivning	Prioritet
1		Kontrollera att bandelarna sitter ihop korrekt.	
2		Kontrollera metallskenan i banan.	
3		Kontrollera att inga hinder finns på banan.	
4		Endast en bil i varje skena.	
5		Kontrollera att det inte finns föremål som kan orsaka kortslutning.	
6		Kontrollera att sensorer är fungerade.	

1.1.2 Kontroll av bilar

Krav	Version	Beskrivning	Prioritet
7		Kontrollera att magneterna inte sitter löst eller lossnat.	
8		Kontrollera att hjulen är väl moterade.	

1.1.3 Aktiviteter för förebyggande av brännskador

Krav	Version	Beskrivning	Prioritet
9		Transformatorn får inte vidröras under drift.	
10		Brandfarlig material får inte ligga i närheten av transformatorn.	
11		T-röd för rengöring av bana får inte förvaras i anslutning till banan under drift.	

1.1.4 Förbjudna zoner

Krav	Version	Beskrivning	Prioritet
12		Det är förbjudet att beträda bordet under körning.	

1.1.5 Styrsystemet

Krav	Version	Beskrivning	Prioritet
13		Det måste gå att koppla in manuell drift omedelbart.	
14		Operatör måste omedelbart kunna aktivera nödstopp under hela driftstiden.	

SRS
Användningsrestriktioner
NFFP

Redaktör: Mattias Krysander
Version: 1.0

Status

Granskad	Krysander	0301??
Godkänd	Krysander	030130

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2003
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
1.0	0301??	Slutlig SRS	Krysander

Innehåll

1 Användningsrestriktioner (SRS)

Syftet för användningsrestriktioner (SRS) är att komplettera vidtagna konstruktionsåtgärder för att förhindra felaktigt handhavande.

1.1 Handhavandeprocedur före uppstart

Krav	Version	Beskrivning	Prioritet
1		Kontrollera att bandelarna sitter ihop korrekt.	
2		Kontrollera metallskenan i banan.	
3		Kontrollera att inga hinder finns på banan.	
4		Kontrollera att det inte finns föremål som kan orsaka kortslutning.	
5		Kontrollera att alla räckena på banan är korrekt monterade.	
6		Kontrollera att sensorer är fungerade.	
7		Kontrollera att magneterna inte sitter löst eller lossnat.	
8		Kontrollera att hjulen är väl moterade.	
9		Kontrollera att eventuellt brandfarligt material avlägsnas från transformatorn.	
10		Kontrollera att T-röd för rengöring av bana är minst en meter från bordet med bilbanan.	
11		Kontrollera att det alltid går att växla, till manuell drift, omedelbart.	

1.2 Handhavanderestriktioner under körning

Krav	Version	Beskrivning	Prioritet
12		Det är förbjudet att beträda bordet under körning.	
13		Transformatorn får inte vidröras under drift.	
14		Operatör måste omedelbart kunna aktivera nödstopp under hela driftstiden.	
15		Endast en bil i varje skena.	
16		Om det luktar brännt måste körningen omedelbart avbrytas och luktkälla identiferas samt felrapporteras.	
17		Alla fel som upptäcks ska rapporteras enligt föreskrifter i FRACAS.	

FRACAS
Felrapporteringssystem
NFFP

Redaktör: Mattias Krysander
Version: 1.0

Status

Granskad	Krysander	030125
Godkänd	Biteus	030130

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2003
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
1.0	030125	Slutlig FRACAS	Krysander

Innehåll

1 Felrapporteringssystem (FRACAS)

Felrapporteringssystemets syfte är att upprätta och upprätthålla ett standardiserat rapporteringssystem under hela systemets livslängd.

Det är viktigt att alla tillbud rapporteras, där människan direkt eller indirekt har påverkat skeendet.

1.1 Ansvarig för FRACAS

Bilbaneansvarig är ansvarig för att upprätta och upprätthålla felrapporteringssystemet.

1.2 Rapporteringsförfarande

Rapportering sker i en felrapporteringspärm vid bilbanan. Allvarliga fel dvs fel som innebär driftsstopp eller risk för personskador ska, förutom att rapporters i pärmen, rapporteras direkt till bilbaneansvarig.

1.3 Instans för analys av felrappoertering

Bilbaneansvarig ansvarar för analys och beslut att införa korrigerande åtgärder. Analysen sker genom att utvärdera felrapporter i pärmen med en driftsmånads mellanrum.

1.4 Format för rapportering

För varje fel ska följande information rapporteras:

1. Konfigurationen på systemet.
2. Operationsbetingelser vid felets uppkomst.
3. Felets art.
4. Felets omfattning.
5. Uppgift om vem som uppmärksammade felet, för att kunna skaffa kompletterande information.
6. Skadades person eller fanns det risk för personskada?
7. Skadades materiel eller fanns det risk för materielskada?

1.5 Arkivering

Alla felrapporter ska arkiveras i ett av arkivskåpen i rum 2E:485.

SV
Säkerhetsverifikation
NFFP

Redaktör: Jonas Biteus
Version: 1.0

Status

Granskad	Jonas Biteus	030110
Godkänd	Krysander	030130

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2002
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
1.0	030110	Version ett	Jonas

Innehåll

1 Inledning

Syftet med säkerhetsanalysen är att bedöma om de krav på säkerhet som ställts har uppfyllts. För att kunna genomföra denna bedömning används SRP (säkerhetsdel i offert), SR-CA (analys av säkerhetskrav) och kunskap från tidigare faser i systemets utveckling, t.ex. FRACAS (felrapporteringssystem). Denna utvärdering är en del i kommande SCA/SAR.

2 Beskrivning

Alla säkerhetskrav ska finnas specificerade så att det är möjligt att specificera hur kravet uppfyllts. Verifikation kan genomföras med anlys, beräkning, demonstration, test, inspektion och granskning.

3 Verifikation

3.1 Krav på aktiviteter för systemsäkerhetsverksamheten

Kraven har klassificerats som skall-krav (utmärkta med prioritet 1) och bör-krav (utmärkta med prioritet 2). De krav som saknar prioritet kan i nuläget ej klassificeras. Samtliga krav utförs enligt beskrivning i H SystSäk.

Krav	Version	Beskrivning	Ver. metod	Resultat
1		Säkerhetskrav i TTEM upprättas.	Granskning	Ok
2		Säkerhetskrav i RFP upprättas.	Granskning	Ok
3		SSPP upprättas.	Granskning	Ok
4		SSWG inrättas.	Granskning	Ok
5		SSRP sker.	Granskning	Ok
6		SRP upprättas.	Granskning	Ok
7		PHL upprättas.	Granskning	Ok
8		PHA upprättas.	Granskning	Ok
9		PHL genomföras.	Granskning	Ok
10		SRCA genomföras.	Granskning	Ok
11		SHA/SSHA genomföras.	Granskning	Ok
12		O&SHA genomföras.	Granskning	Ok
13		TES genomföras.	Granskning	Ok
14		SRS uformas.	Granskning	Ok
15		FRACAS upprättas.	Granskning	Ok
16		SV upprättas.	Granskning	Ok
17		SCA med SAR upprättas.	Granskning	Ok
18		PHST bör upprättas.	Granskning	Ok
19		SS skall upprättas.	Granskning	Ok
20		TSR bör upprättas.	Granskning	Ok
21		SR skall upprättas.	Granskning	Ok
22		RADS bör genomföras.	Granskning	Ok

3.2 Materielkrav

Krav	Version	Beskrivning	Ver. metod	Resultat
23		Självsläckande material ska användas i bana (med kringutrustning, t.ex. räcken) samt i bilar.	Inspektion	Ok
24		Strömförsörjningen till bilbanan ska vara utrustad med säkringar.	Inspektion	Delvis uppfyllt

3.3 Operativt inriktade krav

Krav	Version	Beskrivning	Ver. metod	Resultat
25		Vid körning tolereras maximalt 1 avåkning per 100 körda varv. Med avåkning menas att bilen inte kan fortsätta körningen utan manuella ingrepp.	Granskning, test	Ok
26		Bilarna får endast köras i en riktning. Denna markeras med röd pil på banan vid fyra ställen.	Inspektion	Uppfyllt genom text på banan.
27		Om bilar körs åt fel håll ska styrsystemet avbryta körningen senast när en bil passerat två sensorer.	Inspektion	Ok
28		Vid körning tolereras maximalt 1 allvarlig avåkning per 400 körda varv. Med allvarlig avåkning menas att bilen fullständigt lämnat banan eller att bilen har hamnat upp och ner.	Granskning, test	Ej uppfyllt. Klarar 1/10.
29		Bilarna får inte köras så snabbt att de riskerar att lämna banan och orsaka person- eller större material-skada. Detta gäller även under utvecklingen.	Inspektion	Ej uppfyllt under utvecklingen. Annars ok.
30		Säkerhetsavståndet för användning av systemet är bordskanten eller 0.4 m från bilbanan där bordskanten befinner sig mer än 0.4 m från bilbanan. Med användning menas att bilarna rör sig eller att spänningen till bilbanan inte är noll.	Inspektion	Ej uppfyllt. Kunden accepterade inte detta.

Vad gäller säkerheten delas banan in i tre olika typer av segment: α, β, γ. α-segmentet är den del av banan som är närmst dörren samt den del som är närmast datorn. Dessa segment begränsas av vita markeringar på banan. För α-segment gäller höga säkerhetskrav och höga prestandakrav. Det är segment av banan där en avåkning är katastrofal, men där det samtidigt är viktigt med hög fart.

Notera: Krav 31-35 är icke fullt implementerade varvid säkerhetsdelen delvis är inaktuellt.

Krav	Version	Beskrivning	Ver. metod	Resultat
31		α-segmentet ska avklaras på maximalt $5\,s$ sekunder förutsatt att kollisionsrisk eller avåkningsrisk ej förestår.	-	-
32		Felet på skattningen av hastigheten får som mest vara 3 % under hela α-segmentet.	-	-
33		Maximalt en (1) bil får vara i avsmalningssegmentet av banan vid någon tidpunkt. Avsmalningssegmentet definieras som den del där avsmalningen i banan finns, samt sträckorna fram till närmaste sensordel (framåt och bakåt). Om två bilar befinner sig inom området ska den bil som senast inträdde i området stannas tills dess att maximalt en bil är kvar inom segmentet.	-	-
34		β-segment är de partier av banan som ej ingår i α-segmentet och där avåkning resulterar i avåkning från bordet. Detta definieras som de punkter på banan där bordkanten befinner sig mindre än 20 cm från positionen i rörelseriktningen. För β-segment gäller att vid körning tolereras maximalt 1 avåkning per 1000 varv.	Granskning	1/10 kan uppfyllas
35	Ej säkerhetskritiskt.	I kurvor på β-segment ska hastigheten inte understiga 80% av den hastigheten som får bilarna till en lätt avåkning. Med lätt avåkning menas att bilen befinner sig rättvänd (m.a.p. rörelseriktning) och inte har snurrat (t.ex. upp och ner), samt befinner sig på banan. På β-segmentens raka partier gäller att den minimala hastigheten är den samma som i framförvarande kurva.	-	-

3.4 Konstruktionskrav

Krav	Version	Beskrivning	Ver. metod	Resultat
36		Barriärer ska vara elastiska.	Inspektion	Ok
37		Barriärer ska finnas vid kurvor samt 20 cm efter varje kurvas slut i körriktningen.	Inspektion	Majoriteten ok
38		Barriärer ska vara 2.5 cm höga i lätta kurvor vilket defineras som den minsta kurvvarianten som finns på banan. Övriga barriärer ska vara 5 cm höga.	Inspektion	Majoriteten ok
39		Sensorer på banan får inte kunna orsaka personskador.	Test	Ok
40		Aktuatorer längs banan får inte kunna orsaka personskador.	Test	Ok
41		Programmet får inte innehålla konstruktioner som låser Matlabs kommandotolk mer än 0.05 sekund. Kravet finns av säkerhetsskäl, för att undvika att bilarna kör av banan. Kravet verifieras med tic-toc i Matlab.	Test	Ok.
42		Samtlig mjukvara ska kontrolleras av annan person är programmeraren innan den får användas.	Inspektion	Ok
43		Samtliga kommandon i mjukvara, med undantag för triviala, ska dokumenteras.	Granskning	Ok
44		Varje rad i mjukvaran får utföra maximalt en (1) funktion.	-	-

SCA
Säkerhetsutlåtande för bilbanan i rum 227:118
NFFP

Redaktör: Mattias Krysander
Version: 1.0

Status

Granskad	Krysander	030114
Godkänd	Biteus	030130

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2003
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
1.0	030114	Slutlig SCA	Krysander

Innehåll

1 Säkerhetsutlåtande (SCA), säkerhetsrapport (SAR)

Säkerhetsutlåtandet är ett producentens ställningstagande till systemets säkerhet. Underlag för säkerhetsgodkännande (SS). Det sammanställda underlaget för utlåtandet sammanställs ofta i en säkerhetsrapport (SAR).

2 Systemidentifiering

2.1 Benämning

Systemet benämns: “Fordonssytems bilbana”.
Modellbeteckning: “Mod 01”.

2.2 Systemets omfattning

Systemet består av bilar, bilbana, sensorer, aktuatorer, programvara, I/O-port, kablage, strömförsörjning.

2.3 Avsedd användning

Systemets avsedd användning redovisas i SRS.

3 Underlag

3.1 SSPP och SAR

Kraven på leverantörens genomförande av systemsäkerhetsverksamhet framgår av Systemsäkerhetsplan 2002-08-14. Resultat av systemsäkerhetsverksamhet är dokumenterad i Säkerhetsrapport.

3.2 Tillämpade säkerhetskriterier

De säkerhetskriterier som används vid systemsäkerhetsverksamheten utgörs av beställarens krav enligt Säkerhetskrav i offertförfrågan samt motsvarande punkter i Kravställning i offertförfrågan.

3.3 Klassificering av risker

Vid klassificering av risker har metodikenligt Försvarsmaktens Handbok Systemsäkerhet 1996 utnyttjas, punkt 1.12.3.

4 Genomförd systemsäkerhetsverksamhet

4.1 Identifiering av risker med analys och provning

För identifiering av riskkällor har Preliminär Riskkällelista framtagits. Preliminär riskkälleanalys har genomförts. Här identifierade vådahändelser har analyserats med hjälp av felträd respektive feleffektsanalys.

Analys- och provningsresultat har fortlöpande utnyttjas i konstruktionsarbetet.

Härvid har smatliga enkelfel kunnat elimineras genom omkonstruktion.

4.2 Riskminskande åtgärder

Ett stort antal riskminskande åtgärder har införts och inarbetats i konstruktionen enligt Preliminär riskanalys.

4.3 Tänkbara vådahändelser, kvarvarande risker

Förteckning över tänkbara vådahändelser är framtagna genom analys av preliminär riskkällelista. För varje vådahändelse har identifierats aktuella risker samt har angivits de restriktioner som erfodras till förhinder av olycka.

4.4 Restriktioner

De åtgärder brukaren skall vidtaga för att förhindra olycka redovisas i Användarrestriktioner. Det åligger bilbaneansvarig att noga sätta sig in i dessa restriktioner samt att före självständigt utnyttjande noga utbilda varje person som avses bruka bilbanan.

5 Säkerhetsutlåtande

Fordonssystems bilbana mod 01 är konstruerad efter bästa kunnande. Framtagningsrbetet har stötts av en omfattande systemsäkerhetsverksamhet enligt beställarens fastställda SSPP. För bilbanan har angivits ett antal restriktioner redovisade i Användarrestriktioner.

Fordonssystems bilbana mod 01 är så säker som skäligen kan förväntas under följande förutsättningar:

- Restriktioner i Användarrestriktioner skall noga iakttagas.
- Brukare skall ha genomgått utbildning i handhavande, säkerhetsbestämmelser och vård av bilbanan.

Mattias Krysander

VD Bilbaneinstallatören AB, Linköping

PHST
Regler för hantering, lagring och transport

NFFP

Redaktör: Jonas Biteus
Version: 1.0

Status

Granskad	Jonas Biteus	030110
Godkänd	Mattias Krysander	030130

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2002
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
1.0	030110	Version ett	Jonas

Innehåll

1 Inledning

Syftet med PHST är att tillhandahålla en platform för framställandet av säkerhetsinstruktioner till användare, tillverkare, och alla andra som på något sätt kommer i kontakt med produkten.

Säkerhetsinstruktionerna ska innehålla:

- Regler för hantering och underhåll.
- Regler för användande.
- Regler för lagring.
- Regler för transport.
- Regler för tillvägagångssätt vid inträffat tillbud.

2 Dokumentation

Dokumentationen ska finnas tillgänglig i laboratoriet.

2.1 Regler för hantering och underhåll

- Bilar
  - Före användning ska kontaktdon kontrolleras för oxidation och andra fysiska skador.
  - Före använding ska hjul kontrolleras för sprickor och andra fysiska skador.
- Styrelektronik
  - Endast utbildad personal får utföra förändringar av styrelektronik.
  - Före användande ska kablage kontrolleras för fysiska skador.
- Bana
  - Före användande ska skenor kontrolleras för fysiska skaror, bla oxidation.
  - Metallverktyg får ej användas vid rengöring av banan.
  - Bansegment får endast särkopplas av utbildad personal.

2.2 Regler för användande.

- Användare ska ha läst och följt "Regler för hantering och underhåll" innan start.
- Innan reglersystemet startas ska reglerparametrar dubbelkollas.
- Strömförsörjning ska kopplas ur efter användning.
- Fordonen får ej stannas med fysiska ingrepp.
- Endast ett fordon får befinna sig på varje bana.

2.3 Regler för lagring

- Materialet ska förvaras tort.

2.4 Regler för transport

- Banan ska isärtagas i sekvenser för att minimera arbetet med att sammankoppla delarna.
- Efter transport måste samtlig kablage till styrelektronik och sammankopplande av bandelar dubbelkontrolleras. För att minimera risken för kortslutning och brand.
- Sensordelar ska paketeras som stötkänsligt material.

2.5 Regler för tillvägagångssätt vid inträffat tillbud

- Efter tillbud ska fordon och bana kontrolleras för fysiska skador.
- Vid personskada ska ansvarig för laboratoriet kontaktas.
- Vid allvarlig personskada ska läkare kontaktas.

SS
Säkerhetsutlåtande
NFFP

Redaktör: Jonas Biteus
Version: 1.0

Status

Granskad	Jonas Biteus	030131
Godkänd	Lars Nielsen	030203

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2003
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
1.0	030131	Version ett	Jonas

Innehåll

1 Inledning

Syftet med säkerhetsutlåtandet är att formellt besluta att det producerade systemet är säkert att använda. Detta betyder att säkerhetskraven som ställts på produkten är uppfyllda. Detta innebär bland annat att säkerhetskraven enligt offert är uppfyllda och att lagar och förordningar efterföljs. Fortsättningsvis innebär detta också att systemet har en risknivå som kan accepteras då de uppställda säkerhetsrutinerna efterföljs.

För att kunna göra detta utlåtande används bland annat leverantörens SCA/SAR och PHST.

Denna SS kommer att utgöra ett viktigt dokument då kunden tar beslut om SR.

2 Säkerhetsutlåtande

Med stöd av dokumenten SCA/SAR och PHST samt konsultation med SSWG kan produkten sägas uppfylla de krav på säkerhet som krävs av kund samt lagar och förordningar.

- Bilbana med tillhörande styrsystem accepteras som säkert.

TSR
Användarmanualer och utbildning
NFFP

Redaktör: Mattias Krysander
Version: 1.0

Status

Granskad	Krysander	030131
Godkänd	Krysander	030131

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2003
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
1.0	030131	Slutlig TSR	Krysander

Innehåll

1 Användarmanualer och utbildning (TSR)

Användarmanualer och utbildning (TSR) faställer och utger de instruktioner som erfodras för ett säkert handhavande av system. Indata är säkerhetsgodkännandet (SS) och Förslag till hanterings- och förvaringsbestämmelser (PHST). TSR är en förutsättning för Beslut om användning (SR).

1.1 Manualer med säkerhets- och skyddsinstruktioner

De säkerhets- och skyddsinstruktioner som gäller är de i PHST föreslagna instruktioner.

1.2 Utbildning

Utildningskravet är att kunna samtliga restriktioner som redovisas i Användarrestriktioner (SRS).

SR
Säkerhetsbeslut
NFFP

Redaktör: Jonas Biteus
Version: 1.0

Status

Granskad	Jonas Biteus	030131
Godkänd	Lars Nielsen	030203

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2003
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
1.0	030131	Version ett	Biteus

Innehåll

1 Inledning

Säkerhetsbeslut är den officiella och formella deklarationen av kunden att produkten uppfyller säkerhetskraven samt lagar och förordningar. Beslutet betyder att produkten får användas om den används för sitt definierade syfte och om de regler som uppställts för användande efterföljs.

Beslutet gäller endast den specifika versionen av produkten. Eventuella förändringar av produkten eller dess användningsområde måste följas av ett nytt beslut.

Beslutet baseras på SS från leverantören och under förutsättning att manualer och annat material levereras med produkten. Bland annat ska

- SSWG vara sammansatt och dess uppgift definierad.
- Rutiner för användande, underhåll och säkerhet fastslagits och distribuerats.
- Rutiner för hantering av tillbud fastslagits och distribuerats.

2 Säkerhetsbeslut

Härmed beslutas att produkten är godkänd ur säkerhetssynpunkt för användning.

RADS
Riskanalys för avveckling av system
NFFP

Redaktör: Mattias Krysander
Version: 1.0

Status

Granskad	Krysander	030131
Godkänd	Krysander	030131

Projektidentitet

Projektsnummer:	0201
Årtal-termin:	VT-2003
Projektnamn:	NFFP
Beställare:	Linköpings Tekniska Högskola, ISY, Fordonssystem

Dokumenthistorik

Version	Datum	Utförda förändringar	Granskad
1.0	030131	Slutlig RADS	Krysander

Innehåll

1 Riskanalys för avveckling av system (RADS)

Riskanalys för avveckling av system (RADS) ger endast krav på vilket underlag som alltid skall finns tillgängligt för systemet.

1.1 Underlag

Material som antas ha farliga egenskaper för människa eller miljö ska på ett systematiskt sätt redovisas. För varje sådant ämne ska toxicitet, nedbrytbarhet och restprodukter vid förbränning eller annan destruktion redovisas.

1.2 Konfigurationsstyrning

Bilbaneansvarig ansvarar för systemdokumentation samt uppdatering av ändringar av konfigurationen för att kunna utföra en riskanalys inför avveckling.

1.3 Analys och aktiviteter

Eftersom systemet har utvecklats med stöd av systemsäkerhetsverksamhet bör inte särskilda analyser erfodras.

1.4 Donation

Om helt eller delvis användbart system skall doneras skall eventuella defekter och riskkällor dokumeteras skriftligt och åtfölja objektet.