5 April, 2011

Managing the Risks of Use Errors:

The ITS Warning Systems Case Study

The Technion – Gordon Center for Systems Engineering

Moshe Weiler and Avi Harel

"To err is human…" (Cicero, I century BC); …

"To forgive, divine" (Alexander Pope); …

"To understand the reasons why humans err is science" (Hollnagel, 1993)

To mitigate the risks of human errors is usability engineering

I. Introduction

1. In-Vehicle Collision Avoidance Warning Systems (IVCAWS)

Intelligent Transportation Systems (ITS) provide means to reduce the rate of accidents proactively. Such systems provide car drivers with warnings about multiple potential crash hazards (i.e., forward and side collisions, running off the road, or too aggressive driving). It is hoped that such warning systems may decrease the number and severity of motorist injuries and fatalities.

2. Safety-oriented Design Strategies

Efforts to design safe systems go back at least a hundred years ago. Rigorous and defined approaches to safety engineering mostly arose after WW2.

Safety Management is a combination of two strategies (Doc 9859, 2009):

The Reactive Strategy is a gradual development of the safety requirements, in response to risky events. It is most useful when dealing with technological failures, or unusual events. The level of safety is based on reported safety occurrences, with its inherent limitations, such as: examination of actual failures only; insufficiency of data to determine safety trends; insufficiency of insight regarding the chain of causal and contributory events; the existence and role of latent unsafe conditions.

The Proactive Strategy includes identifying hazards before they materialize into incidents or accidents and taking the necessary actions to reduce the safety risks (i.e., Risk Mitigation Plan). A key action is the validation of risk reduction. Any change in the system involves introducing new risks. How do we prove that modified system is safer?

In the design of warning systems, this implies that we consider all expected circumstances, such as the user awareness of a sensor fault, the user's attention to sound alarms, the user's awareness of a failure of the audio channel, visual backups for the audio channel, testing procedures, etc.

3. The ITS Goals

The ITS industry needs to decide on the best way to select from among the available warning devices and configure them in an IVCAWS. The ITS industry needs answers to the following questions:

- On what conditions should the system alert the driver?
- Which perceptual channel (visual vs. audio) should be used for the alarms?
- How many distinctive alarms can the drivers recognize?
- How to set the alarm thresholds?
- Which sound composition (speech, tonality, tone phrases) are most effective in alerting and in ensuring immediate hazard recognition?
- Which alarm properties (volume, pitch, frequency, direction and location in space) are most effective regarding these tasks?
- How to coordinate the alarms installed by several vendors?
- How to distinguish the road alarms from sounds generated by other devices used in driving (radio, mobile phones, maintenance alarms, …)?

4. The Research Challenge

For many years, engineers strive to avoid accidents caused by system failure. Those preventive actions, however, failed to identify some potential hazards of a safety critical system attributed to limitations of the human perception.

Every new technology introduces new risks. It is not clear that the drivers may perceive the warnings properly, and that they will respond as expected. Every single change in the warning system requires extensive testing to prove that the change results in reducing driving risks. Shinar (2000) demonstrated that even after running expensive tests, we might get wrong conclusions. The validation of any solution, whether it is developed proactively or reactively, requires statistical analysis of real data about risky situations, including near-misses and accidents.

5. The Study Goals

75 percent of car accidents are attributed to human error, 80% of them caused by insufficient driver attention (Salmon et al., 2005). New technologies enable the development of affordable ITS, which may help the drivers in various situations. Among these, various IVCAWS are proposed to alert the driver about unexpected risky situations. Obviously, these warnings are often annoying. Therefore, the public will reject these facilities if their contribution to road safety is not evident. IVCAWS Manufacturers are required to ensure that their systems provide

sufficient warnings, regardless of other warning systems installed in the vehicle. Can the drivers handle coinciding warnings?

This study focuses on the evaluation of the effectiveness of an IVCAWS. The goal of this study is to provide a road map about what research activities are required in order to get answers to the design dilemma listed above.

II. The Usability Risk Management (URM) Framework

6. Operational Risks

An operational risk is, as the name suggests, a risk arising from the execution of a company's business functions, including the risk of loss resulting from inadequate or failed internal processes and systems; human factors; or external events (http://en.wikipedia.org/wiki/Operational_risk). It is a very broad concept which focuses on the risks arising from the people, systems and processes through which a company operates. This term is in contrast to project development risks, which are about the R&D activities, namely, before the system becomes operational.

7. Motivation and Applications

Commercial systems, such as banking

The need to define operational risks was not obvious until recently, due to several critical events such as he near collapse of the U.S. financial system in September 2008. The Basel II Committee on Banking Supervision (Basel II) defines an operational risk as:

> "The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."

Civil Defense

The United States Coast Guard provides the following motivation for considering operational risks (CommandInst 3500.3):

> "Human error causes a significant number of mishaps that have resulted in the loss of personnel, cutters, boats, aircraft, and equipment. Many times faulty risk decisions have placed our personnel at greater risk than necessary".

The Military

US Marines: "Leaders and Marines at all levels use risk management. It applies to all missions and environments across the wide range of Marine Corps operations. Risk management is fundamental in developing confident and competent leaders and units. Proficiency in applying risk management is critical to conserving combat power and resources" (MCI ORM 1-0, 2002).

Transportation

US FAA: "The operational risk management process, as other safety risk management processes, is designed to minimize risks in order to reduce mishaps, preserve assets, and safeguard the health and welfare" (FAA SSH Ch. 15, 2000).

8. Sources of Operational Risks

Operational risks are associated with mishaps. A mishap is typically considered as either a use error or a force majeure:

- A use error is a mishap in which a human operator is involved. Typically, such mishaps are attributed to the failure of the human operator (Dekker, 2007)
- A force majeure is a mishap that does not involve a human being in the chain of events preceding the event.

This study focused on the first type of operational risks, namely, on use errors.

9. Operational Risk Management (ORM)

ORM is a decision-making tool to systematically help identify operational risks and benefits and determine the best courses of action for any given situation (FAA SSH, Ch. 15). ORM is a continual cyclic process intended to help decide whether to accept, mitigate or avoid operational risks (MCI ORM 1-0, 2002). It is used to systematically help:

- Identify and assess operational risks
- Determine the best courses of action for any given situation, by balancing risks arising from operational factors with mission benefits.

The risk management process, as are other safety risk management processes, is designed to minimize risks in order to reduce mishaps, preserve assets, and safeguard the health and welfare (FAA SSH Ch. 15, 2000).

In the context of warning systems, a primary goal of risk management is to compare the risk reduction due to the introduction of a new alarm, with the new risks due to possible failures to provide alarms when they are expected, or due to the possible user's failure to perceive the alarms properly.

10. The URM Model

To examine operational risks we need to examine usability failures. The ORM paradigm provides a framework for classifying *use errors*, and for controlling the system behavior in response to such errors.

The URM model is a tool implementing the ORM concept. It consists of a procedure and methods for managing operational risks. The procedure is of incremental development, each increment consisting of:

- Proactive activities, including:
    1. Operational risk analysis
    2. Safety-oriented design
    3. Evaluation of the risk reduction
- Reactive activities, any of:
    4. Feedback about near misses
    5. Accident investigation

The First Increment

The first increment is the incorporation of a first alarm system, which is successful in terms of risk reduction. To validate it, we need to compare the risks introduced by the alarms with those of driving a vehicle which does not have any alarms.

The Next Increments

The next increments are upgrades to the alarm system. An upgrade may consist of the incorporation of additional sensors, or changes in of the existing configuration, such as changing the alarm threshold. Each improvement in any of the alarm parameters should require a whole development cycle, which should end up in a large-scale field test.

III. Risk Analysis of Driving Alarms

This section lists risks involved in the operation of IVCAWS, and analyzes the capability of various models in supporting proactive safety assurance.

Accident is defined as "an event or sequence of events leading to harm, that is, death, injury, environmental damage, or financial lost". Hazard is defined as the precondition for an accident. The aim of risk management study is to minimize (or eliminate) potential hazards of a system. Until today, there is no "super technique" that can produce state-of-the-art hazard analysis for all kind of systems. While most researchers try to improve the existing techniques, some started to create a different and better approach (http://www.robertsetiadi.net/articles/stamp_analysis.htm).

11. System-centered Analysis

Cause-Effect Analysis

Conventional methods of accident analysis use discrete failure events to identify the cause of accident (Dulac & Leveson, 2004). The idea is that an accident is caused by a root cause. The aim of an analysis is to find out which component of the system can potentially become the root cause of an accident (Fenelon & Hebbron, 1994).

In road safety, a root cause may be a failure of the car, a road bump or another vehicle. Obviously, the cause-effect method is insufficient for analysis of road safety, because the driver has an opportunity to handle the situation. Eventually, we regard the external event as a force majeure, and the challenge is to understand why drivers sometimes fail to handle the event.

Conventional Hazard Analysis

This conventional approach uses event-chain models to provide the process of accident analysis (Leveson et al., 2003). These models generally "explain accidents in terms of multiple failure events, sequenced as a forward chain over time" (Leveson, 2005).

There are three basic types of hazard analysis:

1. Exploratory technique, e.g., HAZOP (Hazard Operability Analysis);
2. Causal technique, e.g., FTA (Fault Tree Analysis);

3. Consequence technique, e.g., FMEA (Failure Modes and Effects Analysis) or FMECA (for Critical elements).

These techniques can be used to support one another to produce a stronger (and more complete) technique of safety engineering (Kazmierczak, 2005).

HAZOP causal model illustrates system failure in diagrams of multiple causes, single effect and multiple consequences. As comparison, causal model of FTA relates multiple causes to single consequence while causal model of FMEA relates single cause with multiple consequences (Fenelon & Hebbron, 1994).

In our study, we explore the effect of various parameters defining the warnings, on a single consequence, which is whether or not the event ended up in an accident. In the exploration, we examine two main effects: the probability of alerting the driver, and the probability of proper hazard recognition.

Operating and Support Hazard Analysis (O&SHA)

The O&SHA identifies hazards/risks occurring during use of the system. It encompasses operating the system (primarily procedural aspects) and the support functions (e.g., maintenance, servicing, overhaul, facilities, equipment, training) that go along with operating the system. Its purpose is to evaluate the effectiveness of procedures in controlling those hazards which were identified as being controlled by procedures, instead of by design, and to ensure that procedures do not introduce new hazards. (FAA SSH Ch. 8, 2000, Section 8.9).

Most safety analyses are directed towards uncovering design problems associated with hardware. This is not the intent of an Operating and Support Hazard Analysis (O&SHA). The purpose of the O&SHA is to identify and evaluate the hazards associated with the environment, personnel, procedures, and equipment involved throughout the operation of a system/element.

O&SHA is applicable to ITS installation procedures, in which the alarm parameters and thresholds are set.

Limitations of Event-chain Models

Event-chain models explain an accident as a linear sequence of events. One event leads to another and causes the accidents in the end.

To prevent an accident, the first event in the sequence (the root cause) of that accident must be found; some efforts need to be made to break that chain. This approach focuses more on system components in the physical form, and has limited capability to explain social and organizational factors, system and

software errors, human errors and adaptation as potential cause of an accident (Leveson, 2004).

The STAMP Model

Conventional cause-effect accident analysis methods often failed to handle complex safety critical systems where accidents can emerge not from few components only, but from the interactions between system components.

The Systems Theoretic Accident Model and Process (STAMP) model provides constrain-based definition of safety, enabling proactive safety assurance based on automatic identification of inter-unit inconsistency (Leveson et al., 2003).

Car drivers are expected to constrain certain parameters, such as headway time, at certain levels. For example, in the UK, the headway time should not be below 0.9 seconds.

Responding to Constrain Violation

A primary concern in driving safety is about automatic vs. manual control. For example, suppose that the car speed exceeds the limit, which defines the constraint. The automatic control may be by reducing the speed, to stay in the allowed range. The manual control is by providing an alarm signal, notifying the driver about the exceptional situation.

Both solutions have their limitations, and the best solution depends on the circumstances. In this study we deal with manual risk control.

12. Human Factors

Historically, the human operator was responsible for enabling successful operation. However, since WW2 it became apparent that the design should consider the limitations of the human body, such as the rate of oxygen in the blood, or the effect of high acceleration (Casey, 1993). Practically, human factors specialists focus on the stages of the user's activity:

- Perceiving the system situation;
- Decision making;
- Execution.

Typically, they focus on understanding user failure in these mental stages, and they propose ways to avoid and work around expected or prominent errors.

In the design of warning systems, such as IVCAWS, the focus is on the driver's perception of the risky situation, and especially on the identification of the source for the alarm.

Driver Task Analysis

Analysis of system operation, such as car driving, may be comprehensive if it is based on the user's task analysis.

The driver's main task is to reach a new location in a time frame. A secondary task is to handle hazards, such as crash and turn-over. To handle a hazard, the driver needs to do:

- Become aware of the new hazard
- Recognize the hazard
- Recall the optional ways to respond
- Evaluate the risks of the various responses
- Decide on the most protective response
- Perform the intended response.

These are the driver's safety tasks. When in relaxed driving, the driver might not notice obvious threats. The warning system may help the driver with the first two tasks in this sequence. Accordingly, the warning system's main task is to alert and notify the driver about the hazard.

Situation Awareness

Warnings are intended to ensure proper driver's situation awareness. If the users are not aware of the situation, they might choose the wrong response.

In our case, suppose that the warning system has sensors for warning against front and rear collision. A driver hearing the front collision alarm should learn to respond by instant breaking. Suppose that a driver who is used to respond to front collision alarm receives a warning about another car approaching too close from behind. If the warning is similar to that of the front collision alarm, the driver might respond incorrectly by pressing the brakes pedal, which worsens the situation.

Inadvertent Driving

After few weeks of driving the car, most of the activities listed above become automatic. A car driver typically performs this sequence in few seconds. The decision of how to respond is made automatically. Evaluation of the risks of the optional responses is short, and the decision is based on prior experience, which is not always proper for the current hazard.

13. Human Errors

The FAA attributes most of the airplane accidents to human errors. The DoD HFACS provides a hierarchical taxonomy of human errors, with Acts at the bottom and Organizational Influences at the top (http://uscg.mil/careercentral/cg113/docs/ergo_hfacs/hfacs.pdf).

The DoD HFACS encompasses various aspects of the user operation. "It is intended for use by all persons who investigate, report, and analyze DoD mishaps, and is particularly tailored to the needs of persons assigned to Interim Safety Boards and formal Safety Investigation".

Limitations of The DoD HFACS

The DoD HFACS assumes that the system design is perfect, and the only source for the use errors is the human operator. For example, the DoD HFACS does not deal with improper design and configuration setting, resulting in missing alarms, or in inappropriate alerting .

Classifying Use Errors

The URM Model characterizes *use errors* in terms of the user's failure to manage a system deficiency. Six categories of *use errors* are described in the URM document:

1. Expected faults with risky results;
2. Expected faults with unexpected results;
3. Expected user errors in identifying risky situations (**this study**);
4. User Errors in handling expected faults;
5. Expected errors in function selection;

6. Unexpected faults, due to operating in exceptional states.

In addition, the model provides guidelines for mitigating the risks of these errors. The guidelines for mitigating these risks were examined by test cases consisting of accident reports obtained by study of well documented accidents and by information from the experience of the Risk Management Working Group (RMWG) at ILTAM/INCOSE_IL (16 examples). One of the RMWG conclusions was that additional test cases should be elaborated. Another conclusion was that the proposed guidelines should be tested in real projects.

Managing Situational Errors

If we assume that the user is responsible for preventing the errors, then practically this means that we do not do much to mitigate the involved risks: we can screen the users, we can educate and train them, but basically, we do not avoid the errors.

Situational models assume that the *use errors* are the result of exceptional situation, with painful results (Hollnagel, 1993). The systemic aspect of such situation is referred to Mode Errors. In this approach we treat safety as a dynamic control problem rather than a component failure problem.

A situational error is due to a trigger, which changes the system state to one which is out of the scope of normal operation. The trigger can be a system fault or a user's error. We can mitigate the risks of situational errors, by avoiding such situations, by continuous coordination and by preparing to respond gracefully.

In the design of warning systems, situational errors are due to missed alarms or to false alarms.

Driving Error Analysis

Systems are operated according to procedures, implementing user tasks. The rate of *user errors* depends on the user's familiarity with the operational procedures and on the user's attention (Rasmussen, 1982). The driver might err in any of the tasks listed above.

14. The Case of Single Alarm Signal

Knowledge Transfer

Consider the situation of a driver who is used to respond to warning signals about a certain risk, when changing to a different vehicle, which does not provide these

signals to the particular risk or provide it with different threshold. The driver might not realize that the situation is risky, because he or she relies on the warning signal, which is absent or not in the same manner as in the other vehicle. In our case, let us think about a family who has two cars, or a firm who has many pool cars, and in some of them there is no reverse warning system, and in some there is but with different thresholds. A driver who changes cars might not realize that the situation is risky.

Missed Alarms

'Missed alarms' is a term referring to risky situation in which the driver does not receive a warning alarm. The result is over-confidence, if the driver's situation awareness depends on the alarm. In case of a sensor or audio fault, or in exceptional situations, the driver might not look for other clues about the risky situation, and consequently, he or she might be unaware of the risk. If the driver can manage without the alarm, then the design may be referred as human fault-tolerant.

As an example, let us assume the common situation of reverse warning system that most of the modern cars have. The warnings are audio (pips – the closer you are to a rear object the frequency of the pip get higher) and visual (numbers in color represent the distance to a rear object in meters, and as closer you are the number should have a more reddish color). A *missed alarm* in this situation means that the driver does not receive any warning, or receive a wrong one. The driver can manage without the alarm, so the design may be referred as human fault-tolerant.

Nuisance

If the alarm system generates alarms when there is no risk justifying the alarms, then the driver regards them as nuisance, and ignores them. Subsequently, the driver might miss alarms due to real threats, resulting in incidents. In order that the warnings are effective, they should be provided just in time.

In our previous example, let us say that instead of starting to warn the driver at 1.5-1.2 meters, it starts at 3.0 meters, or it works even without the transmission in the reverse position.

Signal Detection

Signal detection theory is a means to quantify the ability to discern between signal and noise. Ideally, alarms should correspond to hazard: an alarm should be signaled if and only if there is a real threat. Undesired cases are:

- Missed alarm, when a hazard exists and an alarm is not signaled
- False alarm, when an alarm is signaled although no real hazard exists.

The Alarm-Nuisance Tradeoff

There is a balance between the rate of missed alarms and the rate of false alarms, determined by the alarm threshold. Changing the alarm threshold affects this tradeoff

When the detecting system is a human being, experience, expectations, physiological state (e.g. fatigue) and other factors can affect the threshold applied. For instance, a sentry in wartime will likely detect fainter stimuli than the same sentry in peacetime (http://en.wikipedia.org/wiki/Detection_theory).

15. The Case of Multiple Alarms

The risks involved in multi-warning such systems are:

- The warning sound might confound: the driver might not identify correctly the hazard causing the particular warning. If, for example, the driver responds to a left-lane warning instead of right-lane warning, then the risk increases, instead of decreasing.

- The driver's response to a first warning might result in another warning, resulting in stress or even divergence of the driver's behavior.

Beside the need to support hazard recognition by a particular IVCAWS, there is a problem of vehicles with two warning systems, manufactured by different vendors, each using its own convention.

16. In-context interference

Beside alarms, there are other sounds heard during the driving, generated by passenger conversation, radio, mobile phones, maintenance alarms, etc. These sounds might interfere with the alarms, resulting in false alarms, or in masking.

17. Accountability Analysis

Human Error

In the beginning there was the human being, who invented systems, and had problems operating them. Occasionally, the systems killed the operator and other human being around them. These events were called *Human Errors*.

User Error

As the number of systems invented grew, also grew the rate of accidents, and the public became intolerant of the accidents. The term *Human Error* was not adequate anymore, because it suggested that all human being related to the system, including the stakeholders and the victims might be taken responsible for the errors. This problem was solved by changing to the more adequate term, *User Error*, suggesting that we should blame only people involved in the system's operation.

A typical definition of *User Error* is:

> *A User Error is an error attributed to the human user of a complex system, usually a computer system (but not limited to), in interacting with it.*

This term is problematic for the users, because they are taken accountable for accidents due to design or administrative flaws (Dekker, 2002). For example, aviation authorities often use the term 'pilot error' to describe accidents due to regulation deficiencies. A better approach is to understand why people make errors, in order to defend against them (Norman, 1980).

Accountability in Driving

Consider the situation that the system generates excessive warnings, and the driver disables it to avoid the nuisance. When applying 'old view' practices, we might find the driver accountable, and ignore the need to prevent the nuisance. The 'new view' encourages system-level accountability, which may encourage looking for solutions for the nuisance problem. In our reverse warning system it means, for example, using adaptive threshold design (for different drivers, even in the same car).

Use Error

User advocates have noted that the user action is classified as an error only if the results are painful, implying that it is not the user who should be considered responsible for the errors (Hollnagel, 1993). *'Use Error'* is a recently introduced term, replacing the popular term *'User Error'*. The need for changing the term was because of a common mal-practice of the stakeholders (the responsible organizations, the authorities, journalists) in cases of accidents (Dekker, 2002). Instead of investing in fixing the error-prone design, management attributed the error to the users.

The term *'Use Error'* is used also in recent standards, such as IEC 62366: Application of Risk Management to Medical Devices.

The standard defines *Use Error* as an:

> *"…act or omission of an act that results in a different medical device response than intended by the manufacturer or expected by the user"*

IEC 62366 includes an explanation (Annex A):

> *"This International Standard uses the concept of **use error**. This term was chosen over the more commonly used term of "**human error**" because not all errors associated with the use of medical device are the result of oversight or carelessness of the part of the user of the medical device. Much more commonly, **use errors** are the direct result of **poor user interface design**"*

IV. Designing On-road Alarm

18. System-centered Design

Traditional systems engineering focuses on the system design, considering hardware reliability, disregarding the users. Typical examination of the Trigger-Reaction relationships focuses on the system robustness and resilience to system faults.

In the context of warning systems, system-centered design focus on sensor, sound and display functioning according to the specification, and their reliability. Typically, system-centered design assumes that the users know the designer's expectations about the way the users should use the system. Typically, such design assumes that the users behave perfectly anytime, regarding the operational procedures. Typically, such design disregards common operational conditions, such as user fatigue.

Cause-Effect Design

Common practices for safety assurance are ad-hoc requirements based on cause-effect analysis techniques, such as FMEA, FTA and HAZOP.

In the case of warning systems, the fault tree consists of:

- Sensors;
- Audio channel, used as primary warning means;
- Visual channel, used for testing and for backup of the audio channel.

This kind of design is of limited capability, because it ignores non−linear causality relationships and feedback, and because it is subjective in the choice of events to include. For example, there is no well-defined "start" of the causal chain involved in accidents. As a result, the explanations about the cause for the accident are often superficial (Leveson et al., 2010).

The event chain of vehicle accidents may include situations in which the driver did not notice the visual warnings, because of hardware failure or human factors, and consequently he or she was unaware of failure in the sensors or in the audio channel.

The System of System (SoS) Approach

Systems engineers are often tempted to regard the human operator as an intelligent sub system of a generalized SoS. This approach promotes characterizing the properties and behavior of the human operator.

Theoretically, it enables applying engineering methodologies to the human operator. Conceptually, however, this 'new' system component should be considered as an external constraint: we can consider the human characteristics, but we cannot make the user obey our design.

The implications for the design of warning systems is that we should assume that the users might miss an obvious warning, and provide means to trap such situations.

In IVCAWS design, we should consider the situation in which the users are in stress, or in other mental condition, causing them to disregard the alarms, or to turn them off.

Limitations of the System-Centered Design

Common system-centered practices assume that the users think and behave similarly to the system designers, namely, that they always know and can recall all system states and operational procedures, and the involved risks. Typically, system designers do not anticipate the ways the operators will actually use the system. Often, systems engineers are careless about the system response to exceptional user activity, or about assuring that the user can perceive and correct system faults. Consequently, system designed based on the system-centered approach are typically difficult to operate, and are error-prone (Zonnenshein & Harel, 2009).

In a system-centered design, we assume that the users operate the system according to the instructions. For example, we do not consider the situations in which the users turn off the alarm system, because of the nuisance it generates. System-centered design is insufficient for warning systems, in which the user's perception is critical to safety.

19. ORM Design Principles

Four principles govern all actions associated with operational risk management. These continuously employed principles are applicable before, during and after all tasks and operations, by individuals at all levels of responsibility. (FAA SSH Ch. 15, section 15.2):

- Accept no unnecessary risk:
- Make risk decisions at the appropriate level:
- Accept risk when benefits outweigh the costs:
- Integrate ORM into planning at all levels:

20. Types of ORM

The term Operational Risk Management may be interpreted in two ways:

- Risk management restricted to the system operation. The FAA adopts this interpretation, excluding development activities intended to reduce operational risks (FAA SSH Ch. 15, 2000).
- The management of operational risks, including all development activities intended to reduce operational risks.

This study adopts the wider interpretation, in which the management of operational risks involves developmental activities, such as analysis, design, evaluation and testing.

21. User-Centered Design

When scientists had access to computers, they often found it difficult to understand the rules to communicate with the computer program, or to understand the error messages. Weinberg (1971) has analyzed characteristics of computer programmers, hampering such communication. Shneiderman (1980) proposed guidelines to develop software which is user friendly, and, Norman and Draper (1986) elaborated on the ways to encourage system designers consider the user's perspective. Practically, user-centered design focuses on facilitating initial operation.

When applied to warning systems, the guidelines of user-centered design encourage us to consider the user's cognition: perception, decision making and execution. User-centered design does not guide about hardware faults.

Typical design guidelines overlook the need to notify the users about such faults, and to maintain their attention until they are repaired.

Common User-centered Design Strategies

Typical strategies for safety-oriented design include:

- Avoiding the failures, by error prevention
- Resilience to errors that we cannot avoid by design.

In warning systems, avoidance is rarely an option. Resilience assurance may be achieved by (Harel, 2006):

- Visual feedback about sensor failure;
- Audibility testing (in test mode);
- Validation of human factors by usability testing.

Limitations of User-Centered Design Methodologies

The commonly-accepted, formal definition of usability is:

> *"[Usability refers to] the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use." - ISO 9241-11*

However, common user-centered practices focus on the initial operating stages. For example, it is most unlikely that risks of the unexpected Control position in supertanker steering control, which resulted in the Torrey Canyon accident (Casey, 1993), could be identified in a common usability evaluation.

User-centered methodologies may help mitigate risks known to the usability specialists. However, in typical installations, the knowledge about operational risks is fuzzy and not documented sufficiently to enable implementation of usability solutions. Consequently, major operational risks remain unattended.

When applied to IVCAWS, we need to consider technological barriers to full alarm reliability. Knowledge of the technological limitations is essential to estimating the risks of missed alarm and of the nuisance due to coinciding warnings.

22. URM Design Categories

The URM design includes methods applicable to failures of specific categories. The methods proposed in the URM document for handling *use errors* of these categories are listed in the following table:

Table 1: URM Model Categories

Category	Failure mode	Treatment
1	Expected faults with risky results	A 5-stage procedure.
2	Expected faults with unexpected results	Traditional cause-effect risk analysis; CFMA.
3	**Expected user errors in identifying risky situations**	**Consider the limitations of human perception.**
4	User errors in handling expected faults	Consider the limitations of the human attention.
5	Expected errors in function selection	Scenario-based interaction protocol design.
6	Faults due to operating in exceptional states	Embedded model of the inter-system interaction.

The URM document did not elaborate on these methods, suggesting that they should be elaborated in future research. This research tackles this challenge with respect of the third category, namely, about failure to identify a risky situation.

23. Alarm Management

Alarm management is the application of human factors along with instrumentation engineering and systems thinking to manage the design of an alarm system to increase its usability.

Two problems in usability problem applicable to IVCAWS are

- Nuisance of irrelevant alarm. This problem is typical also of medical alarms
- Alarm flood, or avalanche, when there are too many alarms annunciated. This problem is typical also of control rooms.

Basic Requirements

An alarm can be helpful, and it might generate nuisance, which results in higher risks. It is a challenge of IVCAWS designers to generate helpful alarms only.

In order to provide helpful alarms, the designers should define measures of hazards. In order to avoid nuisance, the designers should define measures of the driver's awareness about the hazard.

These basic requirements are too difficult to obtain. A reasonable compromise is by design based on human factors and by validation based on field testing. The method proposed to implement the basic requirements is by incremental development. The first increment is a minimal configuration, providing warnings about a single hazard.

24. Designing the First Increment

Choosing the Sensor

To decide on the basic configuration, we need to rank the hazards for the vehicle. The statistics that we have now are in favor of warning about potential front collision, and we need to examine available solutions.

Two measures applicable to front collision are the potential (headway) and the actual (front collision) time frame available for the driver to tackle the threat.

The Principle of Action Association

The new risk introduced by the warning system: the drivers might take the wrong action, because they are conditioned (used) to respond in a particular way, which is improper for the current threat (http://en.wikipedia.org/wiki/Classical_conditioning).

The principle of action association states that if different action is required, then the alarm should be distinctive, and this should be tested in usability testing.

Although the two measures above apply to the same threat, the alarm signals about them should be different, and well distinguished if they are installed on the same vehicle, because the driver's reaction to them should not be the same: The best response to headway alarms is by releasing the gas pedal, and the preferred response to front-collision alarms is by braking.

Because the alarms are different, according to the incremental development paradigm, we should examine the effectiveness of each of them individually, and choose the one which is most effective.

Constrain Design

The goal of constrain design is to tackle unexpected situations. When the situation is classified as unexpected, the warning system can provide a warning to the users.

In the case of driving with IVCAWS, the rules may be maximum speed, maximum level of bouncing, or minimal headway. For example, the minimal headway can be set to 2 seconds, as recommended by driving safety authorities, or it may be set to 0.9 seconds, the actual headway measured throughout Europe.

Setting proper constrains is a delicate task. For example, setting the headway to 2 seconds will most likely turn the IVCAWS useless, as the system would generate warning alarms continuously. On the other hand, if the headway threshold is too small, the warning might alert the drivers only after it is too late. We will come to this important issue later in the article.

Setting the Alarm Threshold

The alarm threshold should be set such that when the driver is vigilant and aware of the hazards, it should not generate alarm signals. On the other hand, when the driver is not vigilant, it should generate alarm signals even when the risk is regarded as low.

Adaptive Alarm Threshold

The design may be based on algorithms for deciding if the driver is vigilant. The algorithm may include a definition of vigilance and a response method. For example, if the headway is about 1 second, which is typical of high vigilance, then the system should generate headway alarms only when the headway reduces drastically. On the other hand, if the headway is about 2 seconds, which is typical of easy driving, then the system should alert on reduced speed, headway or forward collision hazard.

Adaptive threshold is also useful to educate the driver to keep safe headway.

Adaptable Threshold

(Enable the driver to change the alarm threshold)? Enable the driver to change the rate of nuisance)

Perception Channel Allocation

Visual perception is directional requires focusing on objects. If the alarm is visual, the driver might miss it. Sound perception is not directional, and hearing is possible even when the eyes are close. Therefore, alarm design is based primarily on sound.

In driving, the visual channel is primarily allocated to the main task, which is driving safely, while the audio channel is free to secondary tasks, such as communicating with the other passengers. For this reason, sound is more proper for alerting than by visual cues.

Earcon Design

An earcon is a brief, distinctive sound used to represent a specific event. They are a common feature of computer operating systems, where a warning or an error message is accompanied by a distinctive tone or combination of tones (http://en.wikipedia.org/wiki/Earcon). Earcons are used for alarms, enabling fast recognition of risky situations.

The main function of the audio channel is alerting. Accordingly, the earcon function should be primarily to alert. The features of alerting earcons are: high, raising volume, pitch, and frequency. The alerting properties of the earcons should be validated in usability testing (Harel, 2006)

25. Designing the next increments

Channel allocation in multi-alarm systems

If the alarm is typical to a well-known single hazard, then the driver may learn to associate the sound alarm to the hazard reliably. However, if the system generates alarms about various hazards, then the system should also provide information about the type of hazard, and its relevant attributes (e.g., its direction).

Studies from other fields indicate that hazard recognition by sound alarms is limited (e.g. Sanderson, 2006). The implication to alarm design is that sound should be used scarcely. If the system provides alarms about various hazards, then the following rules should apply.

- Sound should be used primarily for alerting about immediate risks, while the alarm about potential risks should rely on visual cues. For example, if the system is provided with both headway and front collision alarms, then the front collision alarm should be by sound, while the headway alarm may be by visual indication.

- Sound should be used for alerting only, while the hazard recognition should rely on visual cues.

Deciding on the number of earcon

According to results from studies of medical alarms (Sanderson, 2006), people cannot discriminate effectively more than 3. The requirements to identify hazards immediately may result in reducing this number still further.

The safe decision is to use a single, simple earcon for alerting, and to modify its properties (volume, pitch, frequency) according to the threat.

26. Enforcing Common Alarm Recognition

Usability Standards

To prevent use errors we need to consider human factors. Usability standards are about enabling seamless, safe system operation. Therefore, we should expect that usability standards may help prevent use errors.

Standards can help in two ways:

a. Enforcing good practices

b. Enforcing common system behavior.

Today, vehicle manufacturers can install systems that comply with SAE standards: (http://standards.sae.org/safety/collision-avoidance-systems/standards).

Enforcing Good Design Practices

Enforcing good design practices may secure the proper hazard perception in multi-alarm environments.

The Usability Professional Association identifies two main categories of standards: One category is process oriented, focusing on processes, describing principles and making recommendations for how to achieve a result. For example, IEC 60601-1-6 is a process-oriented standard for assuring the usability of medical systems. The standard requires that the manufacturers of medical systems specify the safety requirements based on risk analysis. The other category is system-oriented, providing detailed specifications, and requirements

that must be met. For example IEC 60601-1-8 is a system-oriented standard, intended to assure the safety of medical alarms.

Limitation of the Good-practice Usability Standards

The good-practice standards provide guidance about technical matters as well as about human factors. However, no standard exists yet that guides how to reduce the nuisance of excessive warnings.

Both standard categories are useful in establishing a user-centered design process or in evaluating the usability of a product. However, process-oriented standards are not effective in risk reduction, because they rely on the quality of the risk analysis, which depends on the skills of the system engineers. For example, IEC 60601-1-8 does not provide guidance and instructions for preventing use errors: instead, it relies on IEC 60601-1-6, which instructs that the manufacturers should design the interaction based on risk analysis.

Enforcing Common System Behavior

Enforcing common system behavior may serve three purposes:

- Resolving conflicts between alarms from different manufacturers
- Disambiguating the alarms from other sounds in the vehicle
- Facilitating and securing the changing the vehicle.

V. Evaluating the Risks of Driving Alarms

New solutions may also introduce new hazards. Often, the new hazards are too risky. In warning system design, the rate of nuisance might be too high, resulting in the users' stress, which might impair their judgment when they need to solve a problem.

This section deals with the evaluation of the benefits vs. the risks of introducing a new IVCAWS.

27. Risk Assessment

The weakness of the ORM model is that it relies on our poor capability to assess the risks of warning systems at design time. Assessment is difficult, because it is practically impossible to

- Formulate driving hazards. We cannot foresee all possible situations that might end up in accidents
- Formulate the way each and every driver may respond to each and every warning signal, in each and every combination of properties (volume, tonality, etc.).

Risk assessment tends to be overly quantitative and reductive. For example, risk assessments ignore qualitative differences among risks. (Shrader-Frechette & Westra, 1997).

Risk assessment consists in an objective evaluation of risk in which assumptions and uncertainties are clearly considered and presented. Part of the difficulty of risk management is that measurement of both of the quantities in which risk assessment is concerned - potential loss and probability of occurrence - can be very difficult to measure. The chance of error in the measurement of these two concepts is large. A risk with a large potential loss and a low probability of occurring is often treated differently from one with a low potential loss and a high likelihood of occurring. In theory, both are of nearly equal priority in dealing with first, but in practice it can be very difficult to manage when faced with the scarcity of resources, especially time, in which to conduct the risk management process (http://en.wikipedia.org/wiki/Risk_assessment).

The conclusion from the discussion above is that the risks of driving alarms should be evaluated by testing.

28. Acceptance Testing

Black-Box Safety Verification

The ultimate method for confirming risk reduction is by field testing. One method of testing is the Black-Box verification (a device, system or object which can be viewed solely in terms of its input, output and transfer characteristics without any knowledge of its internal workings). In the case of IVCAWS, the idea is to install such systems in cars, and count the rate of incidents or accidents with and without the systems. Such a study was reported about an Advanced Break Warning System (ABWS) by Shinar (2000).

Computer-Based Testing

A cheap method for evaluating a warning system is by simulation. For example, the effectiveness of an ABWS was evaluated using a Monte Carlo's computer simulation (Shinar et al., 1997), assuming that the drivers were looking ahead and the headway time was less than 0.9 seconds. The conclusion was that the ABWS was effective. However, such results might be misleading.

For example, the fleet study of the effectiveness of the same ABWS revealed that the improvement is doubtable, and economically insignificant (Shinar, 2000).

29. Diagnostic Testing

White-Box Validation

White-box (also known as: clear box, glass box, transparent box, or structural testing) validation is based on validation of internal structures or workings of the system, as opposed to its functionality (black-box validation). The validation procedure consists of setting a test scenario, then throwing in risky events, and verifying that the system responds gracefully to these events.

In the validation of an IVCAWS, white-box validation can test the flow of events between units during a system level test. In a narrow application, it can be used to test the flow of events between the sensors and the alarms. The focus in this case is on the alarm generation. In a broader application, the events may be triggered by road objects. The focus in this case is on nuisance reduction. When applying a SoS approach, we can also include the driver in the loop, and make that the responses to the warnings contribute to risk reduction.

Usability Testing

To help developers understand the barriers to successful operation, several usability practitioners proposed ways to verify and validate the barriers to user's success. The most popular method for usability testing was in special usability labs, in which the users were observed and recorded while performing assigned tasks. Naturally, this kind of usability practices tends to focus on basic operation in the initial stages (Nielsen, 1993).

Limitations of Usability Testing

Usability testing is based on observing the users while doing their real job. Usability testing is a continuous observation of the system operation, in which an observer identifies situations of operational difficulties, and explores the circumstances for these situations.

Monitoring driving is difficult, because the vehicle is mobile. Special means should be provided to work around this limitation, such as using simulators, or installing special monitoring equipment in the cars.

Simulator-based Testing

A special case of usability testing, applicable to this study, is based on driving simulator. For example, a simulator operated in the Ben-Gurion University, was used to evaluate the effect of marijuana on driving, compared to alcohol (Ronen et al., 2008).

However, these results are arguable, because driving a simulator is different from driving a car, as Daniel Stern discusses in a comment to a report about this experiment in a popular magazine (http://www.popsci.com/cars/article/2009-05/who-drives-better-drunks-or-stoners).

Naturalistic Driving Studies

Ideally, usability testing should be conducted in the real operational environment. This approach is implemented in the PROLOGUE project, in which the IVCAWS under test is installed in selected vehicles.

The ITS-EU Project

This is a running European research (also has been conducted in Israel at Or Yarok, the Association for Safer Driving in Israel) name PROLOGUE - PROmoting real Life Observations for Gaining Understanding of road user behavior in Europe. The main objective of PROLOGUE is to demonstrate the feasibility and usefulness of a large-scale European naturalistic driving study. In

naturalistic driving studies, drivers or riders as well as the environment are observed unobtrusively by means of small cameras and sensors, which are mainly placed inside the car. This approach makes it possible to analyze the interrelationship between road user, vehicle, road and other traffic in normal situations, in conflict situations and in actual collisions. Results will lead to a better understanding of road safety and help to realize an intrinsically safe road transport system, making use of in-car technology, self-explaining roads, driver training, etc. Israel is represented in the PROLOUGUE by Or Yarok and the Technion. The Israeli field trial is aimed at documenting, studying and analyzing driving patterns, driving exposure and **exposure to risk of drivers**, mainly young novice drivers (http://www.oryarok.org.il). Our research was separated from PROLOGUE, and we have fresh data after the EU trial. Also, we have investigated some different issues from what was previously done in the EU project.

ITS Collision Avoidance Data

The data was given to us by Or Yarok (with Dr. Tsippy Lotan permission, the Chief Scientist of Or Yarok). The dates were: from July 1st, 2010 till Oct. 17th, 2010. We have given the data of four drivers, that in their cars they used two technologies: in-vehicle data recorders ("green boxes") and vision-based advanced driver assistance systems. These technologies are developed and manufactured by two Israeli companies: GreenRoad (not included in our research) & MobilEye (AWS 4000), respectively. Also, we have used the data of another Israeli company named TrackTec, that its system was part of the research (mostly kinematic events).

The collected events data and their definitions are according to Table 2, and the Sum of Events is according to Table 3:

Table 2: The Events and definitions

Event Type	Definition
Forward Collision Warning	Approaching forward collision
Headway Warning	No appropriate breaking distance
High Impact X	Erratic braking and accelerating
High Impact Y	Erratic swerving or skidding
Lane Departure Warning	Lane departure with no appropriate signaling.
Speed Duration	Crossing speed threshold

Table 3: Sum of Events

Sum of N (Event)	Column Labels						
Driver	Forward Collision Warning	Headway Warning	High Impact X	High Impact Y	Lane Departure Warning	Speed Duration	Grand Total
A	272	1031	1380	512	173	190	3558
B	301	565	858	624	234	148	2730
C	147	364	(*)	(*)	255	199	965
D	313	1319	2382	299	303	439	5055
Grand Total	**1033**	**3279**	**4620**	**1435**	**965**	**976**	**12308**

(*) The G-sensor of car C seems not to work properly.

We can see that we had in total 12,308 Events.

ITS Collision Avoidance Analysis and Results

The most important analysis that we were looking for was related to the number of Events per time unit. This piece of information was not clear at the beginning of the research as regard to very small time units (i.e., seconds), which means that the driver was exposed to more than one warning in a very short time (e.g., while handling the first event, he or she needs to deal with another one). This phenomenon is very important, since it affects the probability of collision avoidance.

We have arranged the data in quintiles that deployed the data according to Appendix A (all 4 drivers, with their related Events statistics), and the results can be seen in Figures 1-4. In Appendix B

As one can see from the results, the phenomenon did occur, and not just by mere chance, but to all drivers, consistently. For example, for driver A (which has 3,558 events) the 10% Quantile is 7.232 sec. It means that 356 events have happened in approximately 7 sec. interval. The 2.5% Quantile is 2.01 sec. It means that 89 events have happened in approximately 2 sec. interval. This phenomenon repeats itself in all drivers, which believe to be good and safe ones.

Statistical Diagnosis

Statistical methods may be applied to analyze incidents, to identify characteristics of risky system-driver response to threats. An example of statistical base diagnosis of computer software was demonstrated by Harel (2009).

VI. Accident Investigation

30. The Old View

Traditionally, people expect the users to follow the operational instructions, and avoid making errors. In case of a use error, the user is accountable. For example, people expect that nurses respond promptly to all medical alarms, even though most of them are irrelevant. In case of an operational error, the operator is to blame. People expect that operators understand the safety implications of each option that they choose during the operation, in any future operational situation, based on unknown designers' reasoning.

In practice, users often fail to identify exceptional operational situations, to recall the operational instructions, and to predict the system behavior in these situations. Typically, in case of an accident, we accuse the user for negligence, and we accuse the operator for unreasonable operation. We consider the user errors as the source of the accident. In fact, most of the accidents are attributed to user errors. For example, it has been reported that 70-80% of the aviation accidents are due to human errors (Wiegmann and Shappell).

This approach is convenient for safety administrators, because if the user is accountable for the accident, they are not. The problem with this approach is that it inhibits processes of safety improvements. The users' typical response is to think more about their own risks, and less about the interests of the organization, or the public (Kohn). The organization avoids acting to improve safety, because such actions demonstrate the accountability of the safety administrators (Decker, 2006). For example, admitting the design mistake that cause the Airbus 320 accident in Mulhouse Habsheim in 1988 could have prevented the accident in Bangalore, India in 1990 (Casey). In this case, the safety administrators preferred to accuse the pilots instead of exploring the systemic circumstances. Also, accusing members of medical teams for accidents due to risky operational procedure is quite common.

31. The New View

The new view of use errors is that the organization can and should prevent use errors. It is unreasonable to demand that the users avoid making errors, because they cannot. The users behave according to a Human Factors version of Murphy's law: "If the system enables the users to fail, eventually they will".

Use errors should be regarded as symptoms of an organizational deficiency, which enables them, and not the sources for the accident. The Human Factors Engineering approach to preventing user errors is by design, by considering the limitations of the users and the operators. This approach enables learning from incidents: instead of blaming the users, we focus on exploring why they failed, in order to understand how to prevent similar mishaps in the future. Recently, a new methodology for safety culture has been proposed, which defines the accountability of the stakeholders in the organization, such that safety considerations override personal interests (Reason).

32. The Accountability Bias

The New View approach is often criticized for encouraging carelessness during the operation, which might result in accidents. Safety administrators often apply such reasoning to justify setting the system in ways that transfer their accountability to the users, which are risky to the public (Decker, 2007). For example, safety administrators are tempted to set alarm thresholds such that the users are overwhelmed with irrelevant alarms, in order to reduce the risks of missing alarms when needed.

33. Operational Error

The term *Use Error* suggests that the error is the result of temporal conditions. However, from the record of accident investigations it is evident that use errors are enabled by poor design and other incessant operational conditions, imposed by the responsible organization (Reason, 1997).

A systems engineering view of such errors may tackle not only the operation cycles, by also installation, configuration and other activities with long-standing effect of the system safety. The term *'Operational Error'* is preferred since it suggests that we should consider all factors affecting safety during the operation, including both short-term and long-term effects (Doc 9859, 2009).

VII. Feedback about Near Misses

Information about near-misses is essential to preventing accidents due to special circumstances in the road.

There is a need to explore ways to get feedback about near misses. This is beyond the scope of this study.

VIII. Conclusions

34. The Roadmap

This study focused on the evaluation of the effectiveness of an IVCAWS. The goal of this study was to provide a road map about what research activities are required in order to get answers to the design dilemma listed above.

The roadmap proposed includes guidelines for analysis, design and evaluation of IVCAWS, as well as for accident investigation.

35. Main Conclusions

The EU research project plans include comprehensive testing phase, intended to investigate some of these problematic issues. If, as we have shown in this study, multi-alarm IVCAWS are installed regardless of the human factors, then we should expect significant driving errors.

The single most important conclusion from this study is that there are many opportunities for the driver to misinterpret the alarms, and that the risks of misinterpreting the alarms are too high to accept. Therefore, the industry should focus on ways to ensure proper interpretation of alarm signals.

In order to ensure proper interpretation of alarm signals, we need standards. However, in order to decide on a standard, we need to get more data about the effectiveness of various alarm triggering, signals and presentations.

36. Limitations of This Study

It is not clear yet what systems may indeed reduce driving risks, and in what circumstances. There are certain critical knowledge gaps that prevent providing detailed design recommendations. It is not clear yet how to set the alarm threshold for the particular sensors, especially when several sensors are used concurrently. Most likely, each IVCAWS should develop a special measure of nuisance, which is based on various sensors.

37. Applications

Applications to the Design & Evaluation of Warning Systems

When the limitations of the human operators are concerned, the characteristics of warning systems in other industries are similar to those of IVCAWS:

- Cockpits design: it has been observed that pilots often disable the warnings, to avoid their nuisance;

- Control rooms: the accident of the Three Miles Island (TMI) nuclear power plant in 1979 involved failure to identify the source for the failure, due to alarm avalanche;

- Medical treatment: many accidents in hospitals are due to forgetting to turn the alarm on after it has been turned off to avoid the nuisance.

Therefore, at least part of the conclusions from this research may also apply to these industries.

Applications to other Categories of Use Errors

Use errors hamper the effectiveness of other industries, resulting in productivity loss, damage to property, high costs of customer support and customer dissatisfaction. The other industries may benefit from applying the methodology introduced in the URM document, which is demonstrated in this research.

38. What next?

Extensive and expensive validation testing should be conducted to approve each particular IVCAW. It is not clear yet what sensors should be required to include in vehicles participating in field testing.

References

Basel II. Committee on Banking Supervision
http://www.bis.org/publ/bcbsca.htm

Casey, S.M. (1993). *Set Phasers on Stun*, Aegean publishing company, Santa Barbara.

CommandInst 3500.3 (1999). Operational Risk Management. United States Coast Guard, http://www.uscg.mil/directives/ci/3000-3999/Ci_3500_3.pdf

Dekker, S. (2006). *The Field Guide to Understanding Human Error*, Ashgate Publishing Company.

Dekker, S. (2007). *Just Culture: Balancing Safety and Accountability*, Ashgate Publishing Company.

Doc 9859 (2009). Safety Management Manual (SMM). International Civil Aviation Organization (ICAO) (http://www.icao.int/anb/safetymanagement/DOC_9859_FULL_EN.pdf).

FAA-DI-SAFT-105. Operating & Support Hazard Analysis. Office of System Architecture and Investment Analysis (ASD). https://sowgen.faa.gov/dids/OSHA.doc

FAA SSH Ch. 8 (2000). Safety Analysis/Hazard Analysis Tasks, System Safety Handbook. http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/media/Chap8_1200.pdf

FAA SSH Ch. 15 (2000). Operational Risk Management, System Safety Handbook. (http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/media/chap15_1200.pdf

Fenelon, P and Hebbron, B. (1994). Applying HAZOP to software engineering models, Risk Management and Critical Protective Systems.

Rasmussen, J. (1982). Human Errors. A Taxonomy for Describing Human Malfunction in Industrial Installations, Journal of Occupational Accidents, 4, pp. 311-333.

Gilbert, D.T., & Malone, P.S. (1995). *The correspondence bias*. Psychological Bulletin, 117, pp. 21–38.

Harel, A. (2006). Alarm Reliability, User Experience Magazine, Vol. 5, Issue 3.

Harel, A. (2008). Standards for Defending Systems against Interaction Faults, INCOSE International Symposium, Utrecht, The Netherlands.

Harel, A. (2009). Statistical Analysis of the User Experience – Invited talk – 2nd Meeting of isENBIS.

Harel, A. (2010). Whose error is this? Standards for preventing *use errors*. 16th Industrial Management and Engineering Conference, Tel Aviv.

Hollnagel, E. (1993). Human reliability analysis: Context and control, Academic Press.

Jones, E.E. & Harris, V.A. (1967). The attribution of attitudes. *Journal of Experimental Social Psychology*, 3, pp. 1–24.

Kazmierczak, E. (2005). Lecture notes, chapter 7, The University of Melbourne, Australia.

Kohn, L.T., Corrigan, J.M. and Donaldson, M.S. (2000). *To Err Is Human*. Washington, DC: National Academy Press.

Leveson, N. G. (2004). A new accident model for engineering safer systems, Safety Science 42 (Apr., no. 4).

Leveson, N. G., Daouk, M., Dulac, N. and Marais, K. (2003). A systems theoretic approach to safety engineering.

Leveson, N.G., Ishimatsu, T., Thomas, J., Katahira, M., Miyamoto, Y. and Nakao, H. (2010). Modeling and Hazard Analysis using STPA. Fourth IAASS Conference, Huntsville, USA.

MCI ORM 1-0 (2002). Operational Risk management. Marine Corp Institute, Headquarters Marine Corps, Washington, DC. http://www.au.af.mil/au/awc/awcgate/usmc/orm.pdf.

NASA-STD-8719.7 (1998). Chapter 7, Other Hazard Analysis Methodologies. http://www.hq.nasa.gov/office/codeq/871977-c.pdf.

Nielsen, J. (1993). Usability Engineering. http://www.useit.com/jakob/useengbook.html

Norman, D.A. (1980). Why people make mistakes, Reader's Digest, 117, pp. 103-106.

Norman, D.A. and Draper, S. (eds.) (1986). User Centered System Design: New Perspectives on Human-Computer Interaction, Hillsdale, NJ.

Rasmussen, J. (1983). Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models; IEEE Transactions on Systems, Man, and Cybernetics, Vol. SMC-13, No.3, May/June.

Reason, J. T. (1997). Managing the Risks of Organizational Accidents, Ashgate Publishing Limited, England.

Ronen A., Gershon P., Drobiner H., Rabinovich A., Bar-Hamburger R., Mechoulam R., Cassuto Y. & Shinar D. (2008). Effects of THC on driving performance, physiological state and subjective feelings relative to alcohol. Accid Anal Prev. 2008 May; 40(3):926-34. Epub 2007 Nov 26.

Ross, L. (1977). The intuitive psychologist and his shortcomings: Distortions in the attribution process. 'In *L. Berkowitz (Ed.), Advances in experimental social psychology* (vol. 10, pp. 173–220). New York: Academic Press.

Salmon, P. et al. (2005). Human Error and Road Transport, Report No. 256, Accident Research Center, MONASH University, Melbourne, Australia. http://www.monash.edu.au/muarc/reports/muarc256.pdf

Sanderson, P. (2006). Auditory Displays in Healthcare, UX Magazine**.**

Shinar, D. (2000). Fleet study evaluation of an advance brake warning system, Human Factors, v42, Pp. 482-489.

Shneiderman, B. (1980). Software Psychology, Winthrop Publishers.

Shrader-Frechette, K. & Westra, L. (1997). Technology and Values. Lanham, Maryland.

Weiler, M. & Harel. A. (2010). Operational Risk Management. Iltam Workgroup on Risk Management (in Hebrew).

Weiler, M. & Harel. A. (2010).

Weinberg, G. (1971). The Psychology of Computer Programming, Dorset House Books.

Wiegmann and Shappell (1999). Human factors analysis of post-accident data: Applying theoretical taxonomies of human error. *The International Journal of Aviation Psychology*, 1999, 7, pp. 67-81.,

Zonnenshein, A. & Harel, A. (2009). Task-oriented Systems Engineering, INCOSE International Symposium, Singapore.

Appendix A - *Distributions License Plate*

Distribution of the time elapsed (in seconds) between events

Driver Quantiles	A	B	C	D	Mean	STD
100.0%	1701	2581	3040	4563	2971.45	1197.62
99.5%	983	1185	1364	1215	1186.98	157.09
97.5%	630	647	769	701	686.59	62.59
90.0%	311	342	358	355	341.47	21.36
75.0%	165	172	163	161	165.26	4.95
50.0%	65	73	55	58	62.82	8.06
25.0%	22	28	20	22	23.07	3.45
10.0%	7.23	7.20	6.02	6.20	6.66	0.64
2.5%	2.01	1.20	1.01	1.01	1.31	0.48
0.5%	0.20	0.01	0.01	0.01	0.06	0.10
0.0%	0.01	0.01	0.01	0.01	0.01	0.00
Moments						
Mean	126.46	139.46	138.17	137.19	135.32	5.98
Std Dev	169.98	201.71	229.71	230.48	207.97	28.64
Std Err Mean	2.96	4.09	7.89	3.44	4.59	2.25
Upper 95% Mean	132.27	147.47	153.66	143.92	144.33	8.99
Lower 95% Mean	120.65	131.44	122.68	130.45	126.31	5.44
N	3293	2435	847	4501	2769.00	1536.23

Appendix B – The PROLOGUE Data

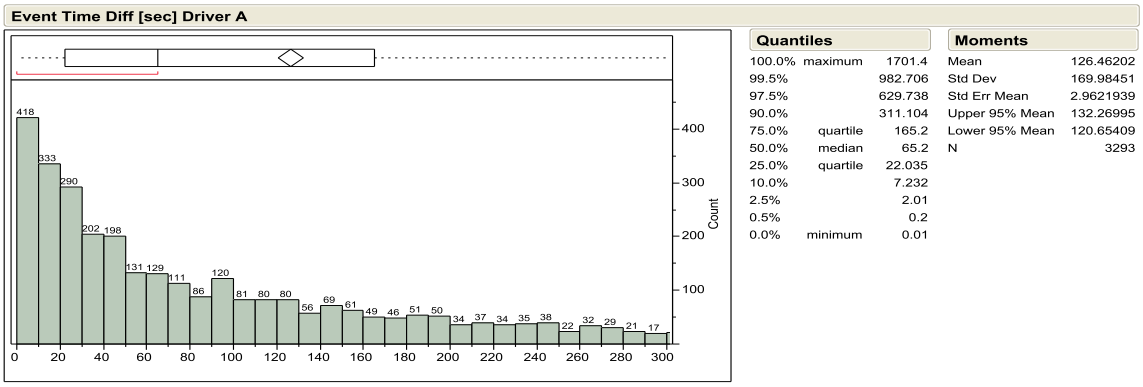

Figure 1: ***Driver A Histogram***

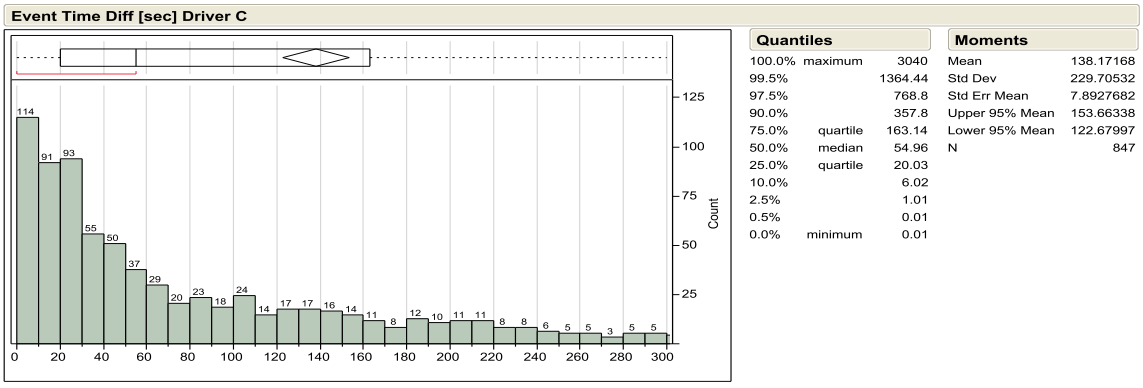

Figure 2: Driver B Histogram

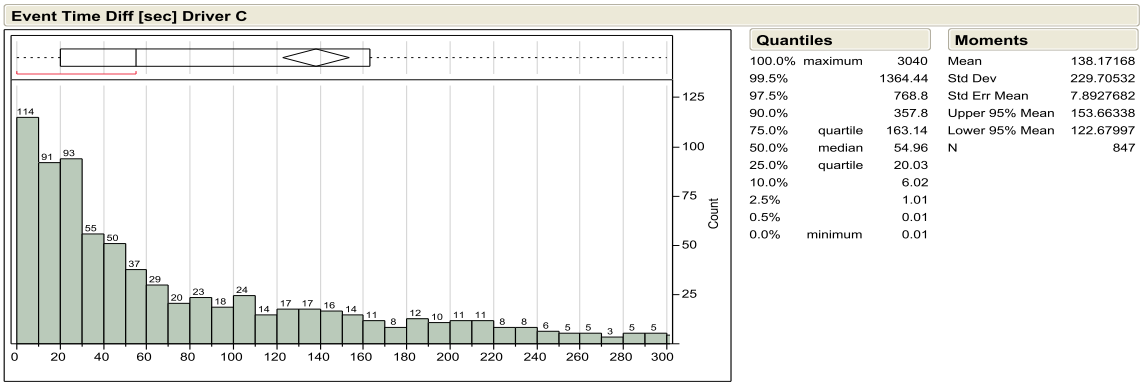

Figure 3: Driver C Histogram

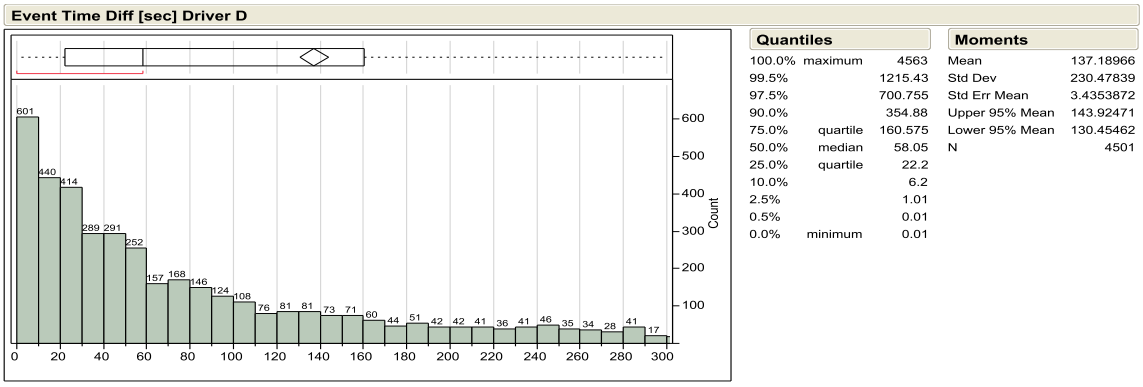

Figure 4: Driver D Histogram