The Israeli Ergonomics Society – 19 January, 2012 – Human Factor Engineering in Military Systems

Designing war alarms
A multi-disciplinary approach

Avi Harel, Ergolight, http://ergolight-sw.com

ergolight@gmail.com

Background

Throughout the short history of Israel, the local population is occasionally exposed to attacks by its neighboring armies and terror groups. The Israeli intelligence provides warnings about possible gun, mortar, rocket or missile attacks, and these warnings are typically communicated to the population via traditional oscillating sirens. The Israeli civilians are instructed to run to a nearby shelter and hide there, or to take an immediate refuge.

Typically, a considerable part of the public responds to the sirens hysterically, and another part ignores them altogether. In a previous study (Harel, 2007) I have analyzed the reasons for the undesired people responses to alarms, and proposed that the alarms should provide additional information to the public. The reasons for the undesired responses include high rate of alarms about hazards irrelevant to the audience, and the confusion about which of the two optional behaviors is the safest. The proposition was that the alarms may be redesigned, to indicate how far will the bomb explode, and when is it expected. In a later presentation (Harel, 2009) I suggested that rather than blaming the victims for not obeying the ambiguous instructions, the authorities should focus on providing the information the public needs about the upcoming hazards.

The article proposes a methodology for evaluating alarm systems, and presents a study evaluating war alarms employing this methodology.

The effectiveness of alarm system

An alarm system may be evaluated by:

- The capability of the alarm generator to generate reliable, comprehendible alarms, and also by
- The capability of the audience to perceive the alarm and to respond properly.

Technology-oriented models typically focus on the alarm generation. User-centered models typically focus on the alarm perception. Human-Factors Engineering (HFE) models should consider both the alarm generation and perception. The focus here is on the effect of the alarm generation on the audience, namely, how the alarms should be generated so that the public may respond properly.

Inter-disciplinary failure analysis

Main sources of alarm failure are beyond the scope of traditional HFE. Predictable failures of system units are typically regarded as problems of System Engineering (SE). Unpredictable, complex failures are typically regarded as problems of the new discipline of resilience engineering (Hollnagel, 2011). Typically, if the outcome is painful, investigators are assigned. Typically, the investigators focus on the behavior of people involved in the failure, and report on particular behavioral patterns that could prevent the failure (Dekker, 2006). If this fails, the investigators may conclude that the failure was a force majeure (Harel & Weiss, 2011).

Extending the scope of Human Factors

This article adopts the holistic approach, considering failure modes attributed to any discipline. The article proposes a Human Factors version of Murphy's law:

> ***If the system enables the users to err, eventually they will!***

Accordingly, system failure may be minimized if the system is designed such that its users cannot fail.

The methodology proposed here is inspired by recent resilience engineering studies, such as STAMP (Leveson, 2004), which demonstrate the need to consider organizational attributes (Reason, 1997) in the design of safety-critical systems.

The study

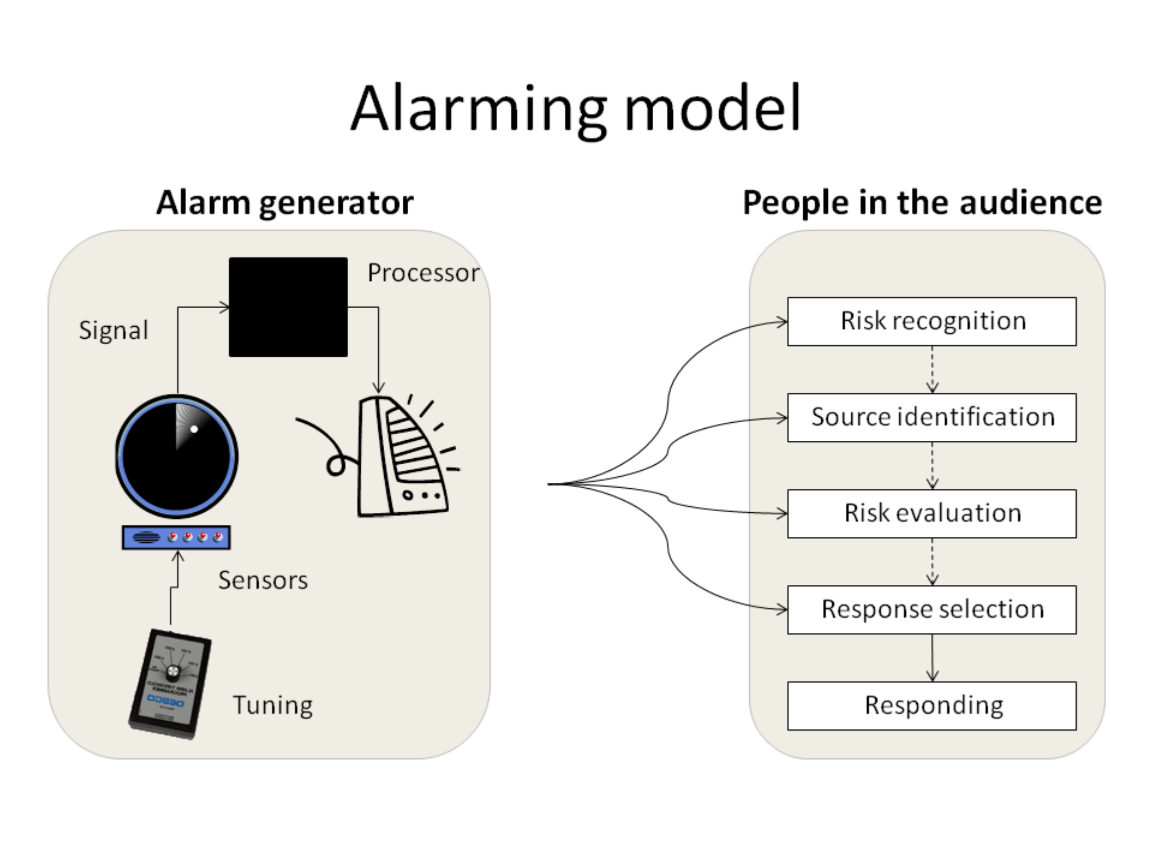
The methodology proposed is based on comparing the requirements from the following alarm systems:

- Military training systems
- Security fences
- Control rooms
- Driving
- Medical monitors

The conclusion was that safety alarms should have common features in terms of the information communicated to the audience, its reliability and the readiness and capability of the audience to correctly perceive the risks, and to respond properly.

A model of an alarm system

An alarm system has two main components: The alarm generator and the audience. The following chart describes a safety-oriented model of an alarm system:



The left side of the model chart describes the equipment and the data flow in the alarm generation, and the right side represents the mental activities of the people in the audience, who need to hear the alarms and respond.

Inter-disciplinary risk analysis of alarm generation

The design considerations applied to assure proper alarm generation include (beside technology) usability, reliability and resilience to failure. Accordingly, the risks involved in the alarm generation are analyzed according to their underlying disciplines, namely, HFE, SE and RE:

HFE risks

Typical risks in the scope of traditional HFE regarding alarm generation include:

- The operator might not notice that a unit is off. This kind of failure is typical of shift changes before a maintenance activity has been completed. This is especially true for maintenance activity about remote sensors, such as missile and rocket launch detectors, of which the operator is not aware. Also, the operator might disable the processor, either intentionally, in order to prevent unintentional activation of an emergency alarm, or unintentionally. This risk is often mitigated by providing visual indicators about the processor being off or disabled. Also, the system may be designed with means to protect from unintentional shutting down of the system units.

- A novice operator might not be familiar with the indications on screen, might not find a critical control, or might fail to follow an operational procedure. Because an alarm generator should almost always remain idle, in normal operation the operators may not have many opportunities to experience the system behavior in emergency. The results might be tragic, as is the case of the 1977 NY city blackout (Casey, 1996a). This risk is often mitigated by periodic on-line training sessions, initiated by the processor.

- The operator might not be sure whether the indication on screen is about a real threat or a phantom. For example, an operator used to respond carelessly to training indications might miss real threats. This risk may be mitigated by ensuring that the indication about real threats is salient and well distinguished from that used for training.

- Undertrained operators, who need to deal with partial, informal or ambiguous operational instructions, are liable to hesitate before deciding to actually invoke an emergency alarm. Hesitation is typical of a first alarm following a long period of tranquility, and is due to being afraid of generating unjustified panic. The tragic accident of Bhopal (Casey, 1996b) was due to this kind of hesitation. This risk may be best mitigated by providing salient warnings about the possible outcome of overriding the system default behavior.

- The operators of a system which is normally idle might not be vigilant at the time when the alarm signal arrives. For example, these were the circumstances of the recent accident of Costa Concordia (http://www.bbc.co.uk/news/world-europe-16620807). This risk may be mitigated by automated alerting of the operators.

SE risks

Typical risks in the scope of system engineering regarding alarm generation include:

- The system might be unavailable, due to lengthy, poorly documented maintenance procedures. This risk may be mitigated by design for maintainability.

- The operator might fail to fix a hardware failure. This risk may be mitigated by integrated troubleshooting software.

- A software bug or a design mistake might result in the system crash. In particular, the system might crash due to insufficient details in the design of the system behavior in cases of exceptional or inconsistent situations. This risk may be mitigated by design and implementation of default system behavior, which includes bug trapping and tracing. Exceptional situations may be captured by employing an interaction protocol (Harel, 2012).

- The operator might be overwhelmed by a high rate of irrelevant alarms, due to insufficient instructions about how to reduce them. This risk may be mitigated by employing the operational procedures instructed in the ISA 18.2 standard.

- Maintenance activities, whether scheduled or occasional might result in unsynchronized events or in an uncoordinated system state. For example, the friendly fire accident in 2001 in Afghanistan was due to changing the battery of the GPS, which was not coordinated with the target acquisition (Casey, 2006). This risk may be mitigated by employing a discipline of continuous coordination (Harel, 2012).

RE risks

Resilience issues include usability, administration and more. Typical risks in the scope of resilience engineering regarding alarm generation include:

- Partial or improper availability of the alarm systems, due to budget constraints, etc. For example, enemy bombs sometimes explode in rural areas, yet most countryside areas do not have any alarm system around them.

- The operator might be constrained by inadequate administrative restrictions. For example, the means necessary to extinguish the Los Alamos fire were provided only after it was getting out of control (Weick and Sutcliffe, 2007).

- The operator might not be sure whether the indicated threat justifies an alarm. This may be the case when the alarm signal does not contain easily accessible information about the significance of the threat, as was in the Bhopal accident (Casey, 1996b). This may also be the case when the operator does not have sufficient information to convince the authorities that an alarm is required, as was in the Chernovil accident.

Inter-disciplinary risk analysis of alarm perception

The right side of the model chart above represents mental activities of the audience. Response issues include hearing problems, people conformity with the alarm and authorities problems in learning from near misses and accident.

HFE risks

Typical risks in the scope of traditional HFE regarding alarm perception include:

- The audience might mistrust the alarm, following instances of missing alarms. Typically, many people respond hysterically to such instances. This risk may be mitigated at the alarm generation, as described above.

- The audience might not hear the alarm due to noise interference. For example, the captain of the AF296 that crashed in 1988 could not hear the alarms, because of the background noise in the earphones. This risk may be mitigated by special electronics that generates test alarm signals and compares them with the ambient noise (Harel, 2006).

- The audience might not recognize the alarm significance. For example, medical teams often fail to recognize the significance of alarms designed according to standards (Sanderson, 2006). This risk may be mitigated by imitating natural alarms (Harel, 2006).

- The audience might fail to estimate the threat, or the risk of disregarding it. Eventually, they might mistrust the alarms. This risk may be mitigated by encoding in the alarms information about the hazard level (Harel, 2007).

- People who feel they need to react do not know what they should do. In war alarms, they might either look for a shelter, or take immediately refuge. This risk may be mitigated by encoding the expected timing of the explosion in the alarm, for example, by variations in the alarm pitch and frequency. Another solution is by replacing the sirens with textual, verbal alarm messages, specifying the time left until the explosion (Harel, 2007).

RE risks

Risks in the scope of resilience engineering regarding alarm perception include:

- The civil defense authorities might disregard data about near misses, for example, by responding to actual accidents only. This risk may be mitigating by assigning officers to collect and analyze data about near misses, and recommend on means to prevent accidents.

- The civil defense authorities might divert the focus of accident investigation to operators or users of the alarm system. The authorities might be in a defensive position about the accident, and consequently they might blame the victims, instead of looking for ways to prevent repeating the accident (Dekker, 2007). This issue may be resolved by adopting the recently developed approach of safety culture.

Conclusion

The design of war alarms should comply with resilience engineering holistic approach, based on analysis of all possible failures.

References

Casey, S. (1996a). An act of God; in S. Casey: *Set Phasers on Stun, And Other True Tales of Design, Technology and Human Error*, Aegean Publishing.

Casey, S. (1996b). Business in Bhopal; in S. Casey: *Set Phasers on Stun, And Other True Tales of Design, Technology and Human Error*, Aegean Publishing.

Casey, S. (2006). Death on call; in S. Casey: *The Atomic Chef, And Other True Tales of Design, Technology and Human Error*, Aegean Publishing.

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

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

Harel, A. (2006). Alarm Reliability: What If an Alarm Goes Off and No One Hears It? *User Experience Magazine: Volume 5, Issue 3* (online: http://ergolight-sw.com/CHI/Company/Articles/Alarm-Reliability.pdf)

Harel, A. (2007). Lessons from the alarm operation in the second war with Lebanon, *The Israeli Conference on Safety Engineering, Ashdod*, (Hebrew: http://ergolight-sw.com/CHI/Company/Articles-Heb/Using-Sirens-In-Lebanon-War-2.pdf).

Harel, A. (2009). Human factors of emergency alarms: the deployment of the lessons from the second war with Lebanon. *The Annual Conference of the Israeli Ergonomics Association*, Kefar Saba, (Hebrew: http://ergolight-sw.com/CHI/Company/Articles-Heb/War-Alarms-2009.pdf).

Harel, A. (2012). Resilience-oriented UML employment. Submitted to the *Israeli Conference of Software Engineering*, Hertzelia, Israel.

Harel, A. & Weiss, M. (2011). Mitigating the Risks of Unexpected Events by Systems Engineering, *The Sixth Conference of INCOSE-IL, Hertzelia*, Israel. (online: http://ergolight-sw.com/CHI/Company/Articles/Weiss-Harel-Managing%20Unexpected%20Events.pdf)

Hollnagel, E., Paries, J., Woods, D. and Wreathall, J. (2011). *Resilience engineering in practice*, Editors, Ashgate.

Leveson, N.G. (2004). A New Accident Model for Engineering Safer Systems, *Safety Science*, Vol. 42, No. 4, pp. 237-270.

Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Aldershot, England: Ashgate.

Sanderson, P., 2006, Auditory displays in healthcare, *User Experience Magazine: Volume 5, Issue 3*

Weick, K.E. & Sutcliffe, K.M. 2007. *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*. Wiley and Sons.