



The Human Resource in Security

A White Paper from the EuroTech Security Group

2009-09-30

Preface

This paper was written on behalf of the EuroTech Security Group by Tor Olav Grøtan, Camilla K. Tveiten, and Lars Bodsberg, SINTEF, and Elina Pietikäinen, VTT.

The purpose of the paper is to argue for a new research topic to be addressed by the EU Security Programme.

Introduction

The overall idea behind this paper is to investigate research topics to mobilize the human factor as a resource for security.

Most European security research programmes have addressed human as threat or contributing factor to loss of security.

A new research approach in security is required to treat human variability as a resource.

A new research approach is required in the way we treat the variability in human behaviour. Human variability is also a resource and the reason why systems survive its threat.

Terminology



In many languages, safety and security are used as synonyms. Safety stems from French and describes the state of being “safe”, the condition of being protected against different types of consequences of failure, damage, accidents and harm. The word Security stems from Ancient Greek and describes the state of being secure; to be without fear or harm. In our world, security is generally used to

express protection against threats that include hostile, intentional acts of will and terror, whereas the concept of safety seldom includes negative acts of will.

In this text, security includes safety, by being something that is done or built/constructed in order to ensure the safety of human beings (and the environment). Vicious acts of will such as terror and hacking or spreading viruses are among the threats to safety that must be accounted for.

What is the problem?

Individuals and organizations influence security through how they maintain and operate socio-technical systems, and through their capacity to handle contingencies. The term socio-technical system is used to describe a system consisting of human and technological factors, sometimes also as being interwoven as in 'joint cognitive systems'¹.

To progress on the issue of human factors in security, we may seek inspiration from the safety science literature on the ways humans, technologies and organizations are dynamically interwoven.

An extensive body of safety research exists concerning human-machine interaction at the individual level. Sociologically oriented researchers have proposed theories that link accidents to the structural properties of organisations², theories that explain outstanding safety performance in complex systems³ and theories that explain major accidents in terms of organizational information processing deficiencies⁴. Furthermore, multi-level analyses, explaining a single accident by integrating phenomena at the individual, group and organisational level, are found in the safety research literature⁵.

Some recent safety studies have aimed at giving human and organizational contributions to resilience at least the same attention as human and organizational contributions to vulnerability. Apparently, vulnerabilities, as well as resilience, may arise from interactions between socio-technical system levels.

The processes that create resilience and vulnerabilities cut across traditional disciplinary barriers, such as those between political science, sociology, psychology and engineering⁶.

Human and organizational contributions to resilience should be given at least the same attention as human and organizational contributions to vulnerability.

¹ See Hollnagel, E. and D. D. Woods (2005). Joint cognitive systems: Foundations of cognitive systems engineering. Boca Raton, Fla., Taylor & Francis

² Perrow, C. (1984): Normal Accidents. New York: Basic Books.

³ LaPorte, T. R. and Consolini, P.M. (1991): Working in practice but not in theory: Theoretical challenges of "High-Reliability Organisations".

⁴ Turner, B. A., Pidgeon, N. F. (1997): Man-made disasters. 2nd ed. London: Butterworth-Heinemann.

⁵ An example is Snook, S.A. (2002): Friendly Fire. Princeton: Princeton University Press.

⁶ Rasmussen, R. (1997): "Risk management in a dynamic society: A modelling problem. *Safety Science*, **27**:183-213.

The “positive human turn” in safety science

In order to understand the human factor in any environment, one must have comprehensive knowledge about human cognition, actions and reactions. Humans are more than barely formed by the rules, possibilities and constraints in the systems we act in; some human traits are quite general and come to light in different situations if applicable.

The ‘rational human’ that acts according to a rational decision based on information of all possible alternatives and outcomes of the situation is unlikely to be real. Human rationality is more likely to be ‘bounded’. Human beings do not decide how to behave and act based on calculations of alternatives and consequences; humans apply heuristics and other approximate computations in any decision, conscious or unconscious, and preferences are not static.

Humans are never completely informed of all alternatives and the time to think and act will be limited.

The reasons why decisions are bounded are linked to the facts that the decision maker is never completely informed of all alternatives and outcomes; is unable of discriminating between even the known alternatives, and is unable to rank the alternatives according to criterions. Even if a rational decision is desirable and something the human wants to achieve, the time to think and the time to do will be limited. In any situation, human beings are faced with constrained time and must balance the time spent on thinking about the challenge and acting on the decision. In non-malicious behaviour, the decided act will always aim at achieving a positive or successful outcome, no matter what the actual outcome might be.

Modern systems are so complex that they will always be underspecified. Thus, the decisions taken based on information from the system will always be approximate. There are also many social phenomena in organizations that have an effect on how people make decisions and act in relation to safety or security. For example normalization of deviance refers to a process where potential danger signals slowly become interpreted as part of normal work in the work community and are thus not considered as sings of danger anymore⁷. Creation and maintaining of social identity⁸ is also an important driver for behaviour. Social identity can either promote safety or security conscious behaviour or act against it. For example strong social identity can prevent critical reflexivity towards the actions of one’s own group. All in all

⁷ Vaughan, D. (1996): *The Challenger launch decision*. Chicago, University of Chicago Press, 1996.

⁸ Haslam, S.A. (2004). *Psychology in organizations. The social identity approach*. Second edition. London: Sage.

the collective sense making⁹ about the meaning of different events that goes on among humans guides the behaviour in the organization and affects safety and security.

Human action will be adjusted to the situation - humans are unable to act the same way according to instructions in all situations.

In order to detect deviations in any system, humans must know the system and have experience with the behaviour of the system. For instance, a person that knows the behaviour of a company and thus knows that the company never call for personal information by using e-mails will be a very good detector of abnormal behaviour. He or she may avoid responding to a demand for personal information and even warn the company of the security threat. In any system, the borders of the socio-technical system are difficult to draw. The customers in a company and their computers and other technology they use, will in most cases belong to the system and should be included in any strategies for ensuring safety and security of that system.

It is impossible to expect behaviour of humans in a system to follow all rules or to fit into all the official normative roles. Humans will seek to optimize behaviour in any system in order to ensure positive outcomes. From this it follows that humans are unable to act the same way according to instructions in all situations; human action will be adjusted to the situation, level of alert will be different and attention will be drawn to what seems most important in order to ensure success at the time.

Within safety research, there has been a 'positive turn'. In this view, human variability is a resource.

This knowledge of human variability and organizational phenomena has been taken into account for the belief that human beings are error prone and their performance must be controlled and constrained. One of the problems with this solution is that human beings react to constraints by applying the same adjusting behaviour; and by this constructing a very different outcome than what was expected. Within safety research, many have reacted to the view of humans as erroneous and called for a 'positive turn' in the way we treat the variability in human behaviour. In this view, human variability is a resource and the reason why a system survives its threat, though sometimes the combined variability in the system may have unwanted outcomes in special situations.

⁹ Weick, K.E. (1995): Sensemaking in organizations. Thousands Oaks: Sage.



An uncontrolled release of gas occurred at Snorre A (2004) - an offshore oil and gas production installation on the Norwegian continental shelf. The potential consequences of an uncontrolled, ignited and burning gas blow-out were huge. Although there were no detailed procedures for handling this particular scenario, the situation was successfully recovered through the way in which the platform crew handled this crisis situation

The human factor as a resource requires a reflexive attitude and practice

The human must understand his/her own role in protecting the system as a whole, recognizing that he/she may be used as a point of leverage by a hostile agent/agency. The organization must attend to creating and maintaining this understanding among its personnel. The organization needs to take care of necessary preconditions (procedures, information, resources, tools etc.) that allow for this understanding to be created and allow the personnel to act according to their understanding.

A great challenge for humans and the organization as a whole is to anticipate what may happen, what kind of leverage points may be utilized, and how their use may be identified and countered, thereby reconciling security.

By developing scenarios in risk analyses, enterprises may be able to foresee what may happen, and how they can be countered. Research is needed to identify key scenarios, that can be elaborated and provide a basis for more specific scenarios at the organizational level. At the same time it is important to keep in mind that all the possible risks in a complex socio-technical system may never be recognized. It is important to stay mindful and alert for possible new challenges¹⁰.

¹⁰ Weick, K., & Sutcliffe, K. (2001). *Managing the unexpected. Assuring high performance in an age of complexity*. San Francisco: Jossey-Bass.

Some key questions to be addressed concerning human and organizational factors in security are:

- How can intrinsic defences be attacked and weakened as a result of hostile actions?
- How can humans detect hostile actions?
- How can humans counter hostile actions?
- How can organizations create good preconditions for the work of their personnel from a security point of view?
- How can organizations evaluate their level of security, also paying due attention to the positive human contribution?
- What and how can organizations learn from security problems that have already emerged?

A key premise for research addressing and identifying such scenarios is to employ a holistic approach considering human, technology and organization in an integrated manner.

The crucial point, in a security perspective, will be to disclose the double role of humans, both as leverage points of attack, and as barrier/protector. Moreover, research is needed in order to see the implications for preparation, training and simulation in order to mobilize the human factor as a resource in security.

The paths to such research may vary, but safety science already employs a great variety of perspectives that offers a point of departure.

The development of new perspectives in safety research

The development of new perspectives in safety research has influenced the view of human and organizational factors in different ways. In some perspectives, “human factors” are considered a threat; in others a challenge. The positive turn on human factors is most evident in the latest contribution (Resilience Engineering).

Safety science operates with comparatively more frames of understanding its subject matter, than security.

Accident models have a dual role; they are analytical tools for retrospective understanding of accidents and incidents, but they also function as (normative) action schemes with the purpose of preventing future accidents to happen.

*What may go right
despite surprise?*



*What can go wrong
despite absence of
failure?*



What can fail?

Security as a science is still trying to make the barrier “perfect” without questioning the contribution the barrier might have on e.g. the complexity of the system it is supposed to protect.

Very broadly speaking, accident models have had a progression starting with asking the question what (which component, technical or human) can fail, proceeding with the question of what can go wrong despite absence of failure, and proceeding further with what may go right despite surprise and unexpected variation in system behaviour. We can see that the progression stems from a process of discovering that fundamentally new questions may have to be asked in order to find feasible answers.

When barriers were introduced into the Heinrich’s (1931) domino model, we could actually manage the probable outcomes. Reason’s (1997) model of organizational accidents, in which also latent (human, organizational) conditions for barrier breaches are taken into account, opened the door for the contribution from social sciences. However, the wisdom of successive layers of barriers was seriously questioned by Perrow (1984) who claimed that adding more barriers and safeguards, will only make the system more complex, and thus add to the damage already done. With Perrow, the question “what may go wrong despite the absence of failure”, really stepped into the forefront.

By comparison; security as a science is still trying to make the barrier “perfect” without questioning the contribution the barrier might have on e.g. the complexity of the system it is supposed to protect.

The schools of High Reliability Organizations (HRO) and more recently, Resilience Engineering (RE) changes the key question into the following: What may go right despite surprise and unexpected variation in system behaviour?

A new research topic – The human resource in security

Perspectives of human factors in security seem to concentrate on human as a threat and how to control this threat by use of barriers and constraints of behaviour. The challenges with more complex socio-technical systems and modern technology can not be met with traditional view of the human as a vulnerable burden and threat. The task is to develop new perspectives on human and organizational factors in security in which human variability is considered a resource and the reason why systems survive its threat. A key premise for research addressing and identifying such scenarios is to employ a holistic approach considering human, technology and organization in an integrated manner. The crucial point, in a security perspective, will be to disclose

the double role of humans, both as leverage points of attack, and as barrier/protector.

The main goals for research are:

- To define a roadmap to stimulate the existing adaptive practices that constitutes human variability as a resource.
- To develop a reference framework for security means which also includes humans as a resource in security as individuals and as part of society.
- To investigate how the experiences with the positive human turn of safety can be combined with security.
- To establish European guidelines for incorporating human reflexivity in planning, training and simulation.
- To exemplify new organisational approaches that include human as a resource within security management perspectives.
 - To describe the characteristics of an organization with good security or security culture.
 - To develop a model for evaluating the level of security in an organization.
 - To develop a model that helps organizations to learn from security problems that have already emerged.