Architecture-based Model for Preventive and Operative Crisis Management

Erland Jungert, Gunilla Derefeldt, Jonas Hallberg, Niklas Hallberg, Amund Hunstad, Ronny Thurén
FOI (Swedish Defence Research Agency)
Box 1165, S-582 26 Linköping
Sweden

jungert@foi.se, gunillad@foi.se, jonhal@foi.se, nikha@foi.se, amund@foi.se, ronthu@foi.se

ABSTRACT

Crisis management will generally engage a large number of actors, working in stressful situations. These actors need to be able to communicate, exchange information as well as gather information, from the area of operations, where ongoing events relate directly or indirectly to the crises. The actors must also be able to give orders to control the situation at hand. All these activities will relate to a large number of more or less complex problems such as large data flows from various data sources. Thus, for instance, means for analysis of incoming data and data fusion must be available. A system that should support activities of this type must not only have a high capacity, with respect to the dataflow, but also have suitable tools for decision support. To overcome these problems, an architecture for preventive and operative crisis management is proposed. The architecture is based on models for command and control, but also for risk analysis.

1. INTRODUCTION

Modern society and its communities are heavily and increasingly dependent on a variety of critical functions and technical infrastructures, supporting for example power and water supply, telecommunications, financial services, public health and transportation. There is also a growing interdependency between the different critical functions and technical infrastructures, caused by tighter integration of the systems and businesses dependent of them. The disadvantage of this, by all means necessary, integration and interdependency, is growing vulnerabilities. Major disruptions can by cascading effects lead to substantial economic consequences or even loss of life and property. Attacks on critical infrastructures may even pose a threat to national security.

The increasing interdependency and integration results in high complexity in the command and control systems needed to support crisis management. To be able to sufficiently protect individuals, communities and society preventive and operative measures have to be designed, implemented and maintained in these systems. A holistic view, incorporating knowledge from a number of research areas, is needed in the development for the proposed function of command and control for crisis management. To handle the high complexity it is crucial to consider all relevant aspects of command and control, such as human factors, decision support and security, from the beginning of the development phase.

Graser et al. [1] describes a system called ENCOMPASS with the purpose to support decision support at a top level of crisis management, e.g. terror attacks. This system uses a type of map based situation analysis that includes check lists for epidemiological surveillance. Rodrigues et al. [2] have developed a system called Mercury with the main purpose to support users at crisis control centrals in integration of data from

Paper presented at the RTO SCI Symposium on "Systems, Concepts and Integration (SCI) Methods and Technologies for Defence Against Terrorism," held in London, United Kingdom, 25-27 October 2004, and published in RTO-MP-SCI-158.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
25 OCT 2004	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Architecture-based Model for Preventive and Operative Crisis Management	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **FOI (Swedish Defence Research Agency) Box 1165, S-582 26 Linköping Sweden**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM201977, Systems, Concepts and Integration Methods and Technologies for Defence against Terrorism (Systemes, concepts, methodes d'integration et technologies pour la luttre contre le terrorisme)., The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**12**	

many different systems. The main research objective is to develop a suitable architecture for crisis management. PRESTO [3] is focusing on the human aspects of distributed system for crisis management in which cooperative work plays a fundamental role in a system based on an architecture for multimedia information. A system related to a C^3-system, i.e. for command, control and communication, for crisis management is discussed in [4]. Other work that relates fairly well to the work discussed here can also be found in [5][6][7].

In chapter 2 the main objectives of the described approach is stated and in chapter 3 the methods used in the work. In chapter 4 a proposed crisis management architecture, consisting of a command and control model, risk model and a command and control system, is described. Important research areas to enable such an architecture and its system development, is discussed in chapter 5. Conclusions of the research work so far are stated in chapter 6.

2. OBJECTIVES

Of main concern in crisis management is generally that an often large number of actors are engaged in applications where they must be able to communicate, exchange information but also to gather information about the ongoing events related directly or indirectly to the actual crises. The actors must also be able to give orders to the personnel actively working in the area of operations. Especially, the flow of data that is coming in from the field is not only large but of complex type as well. Consequently, means for operations like analysis, data fusion and storage of these data must be at hand. The capacity of the dataflow and the tools designed to support the manipulation of the data must be high, that is real time or close to real time capability is required. Considering this, and the clearly stressful situation that the users have to deal with, some type of information system that can help the users to overcome these obstacles must be available. Given the above requirements the objective must be to develop a functionality for command and control that includes means for both preventive and operative actions.

3. METHODS

Targeting the objective of this paper, to explore a model-based architecture for preventive and operative crisis management, a project group was constituted including six researchers with different specialties related to the development of C^2 –systems. Those specialties were; (1) decision support systems and query languages, (2) system architecture, (3) systems development, (4) IT-security, (5) human-system interaction (HIS), and (6) human factors. To the work of those six researchers, six additional researchers with complementary specialties were engaged to contribute to the work. Their specialties were (7) management, (8) communication, (9) sensors, (10) situation awareness, (11) threat structure and, (12) training and evaluation.

The project group met regularly during a period of six mouths, with the aim to develop models for C^2 -systems, to be used in the domain of preventive and operative crisis management. The work was based on a top-down strategy, where an initial high-level model was developed, based on scenarios and a C^2-model suggested by Worm [8]. The outcome of this initial work was an abstract model of C^2 for threats and crises. The C^2-model was evaluated and modified in several steps, based on the specialties of all participating researchers. During this part of the work, the need for more detailed models on lower levels was explored. Several models were constructed, but in this paper only the risk model are presented in addition to the C^2-model.

4. THE CRISIS MANAGEMENT ARCHITECTURE

Complex information systems, like command and control systems for crisis management, must be based on an architecture that is flexible with respect to such requirements as generality, modularity and

expandability. There are also other aspects that must be considered when designing modern information systems of this kind. These systems must be able to include means for detection and identification of objects as well as for storage and manipulation of these objects. Clearly, threat assessment must also be part of these activities since in many cases the objects of concern correspond to threats. As a consequence, the underlying architecture must be based on an appropriate approach. In this work, the approach taken is model-based, that is two fundamental architectural models, that together can serve as a framework for the final command and control system, have been identified. The two models are interrelated. The first one constitutes a command and control model while the second is a risk model that will, e.g. through simulation, be able to judge risks that may be caused by various types of threats. A C^2-model must include various decision support tools and of concern when designing the final system is also to consider most aspects of IT-security. The motivation for the latter is that it will cause serious problems if those design aspects should be considered later on the design phase. The two models, which need to be tightly coupled, will subsequently be discussed further. The relationships between the C^2-model, the risk model and the final command and control system are briefly illustrated in figure 1.

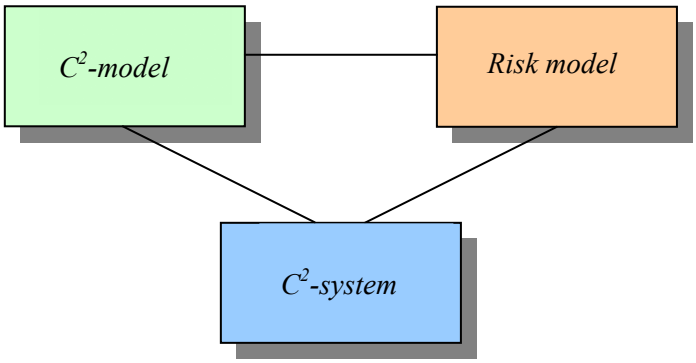

Figure 1. The command and control model, the risk model and the command and control system.

4.1 The C^2-model

The overall structure of the C^2-model can be seen in figure 2. The model is centred around an area of operations. Such an area corresponds to either a space inside which a crisis is going on or where the risk for a crisis is at hand. Thus the area of operation can be subject to both operative and preventive activities. The area of operation is continuously watched over by means of sensors and observers that may be human. The assessment of the area of operations will create very large data volumes. The data must be analysed with respect to the information requested by the users of the command and control system. The analysis is performed in what here is called the surveillance system. However, active in the area of operation may also be what here are called threat agents. The threat agents can, for instance, be different types of terrorists and it is the purpose of the command and control system to support the user in the process of identifying and catching these threat agents. Threat agents can be seen as free agents that leave trails in the area of operation and it is the purpose of the C^2-system to help identify and handle these agents by searching the area of operation for the trails they have left. Clearly, this not the only application of the command and control system but this example is probably one of the more complex.

The information flow that is coming into the system is first sent to a supervising subsystem. The supervising system, which can be seen as the heart of the complete command and control system, may be run by a number of users. However, the supervising system does not in itself constitute the complete command and control system; other partners must be involved, as well, to accomplish the complete system. The other partners are various organizations and agencies, such as the police, the fire brigade and different specialists engaged in the ongoing operations. Information needed by these partners will be sent

to them by the supervising system. However, the partners may also have their own means for data selection because they are actively engaged in the operations in the area of operations. This information can be shared between all or most of the other participants of the operations. Consequently, all the participants of the operations must cooperate to successfully bring the operations to an end. Physically this must be carried out by means of a communication network.

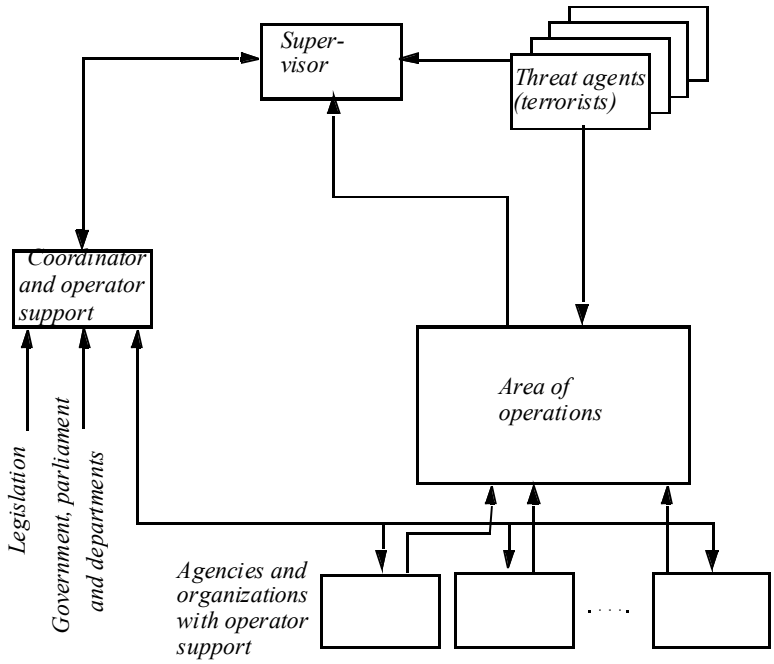

Figure 2. The structure of the command and control model.

The nodes in the required communication network must be equipped with a number of resources. Examples of such resources are illustrated in figure 3. The resources of interest correspond to a set of decision support tools that may vary from one node to another depending on the user's particular needs. The decision support tools use input from the data sources attached to the surveillance system, see figure 2. Besides the input data sources, different a priori databases are also attached. The output information of the decision support tools will basically be used to generate the structural information for visualization in the common operational picture (COP). All the tools are together with the COP attached to a visual user interface from which a user can control the different tools. Furthermore, it must be pointed out that data collected from external data sources quite often will be of heterogeneous types, i.e. the data are coming from multiple sensors and/or human sources. The data will in most cases include uncertainties that are due to limitations in the data sources and for this reason data must be subject not just to ordinary analysis but to (multi-sensor) data fusion [9], as well.

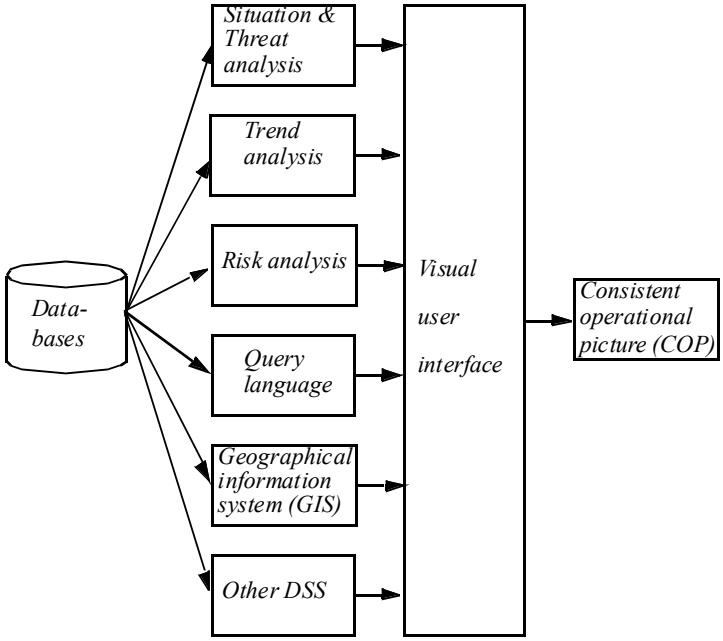

Figure 3. The structure of the operator support of the command and control model including some example of decision support tools.

The command and control system must be modular with respect to the fairly large number of decision support tools that will be needed. In most cases they are designed to support the COP. Among the most important ones that can be mentioned are a geographical information system, a system for data mining [10] (primarily applied to spatial/temporal data) and a system applied to crisis management. A query language for sensor heterogeneous data sources is also required; see e.g. [11] or [12]. Other decision support tools that will be required should focus on situation and impact analysis [9] and also for risk analysis, which will be discussed further below in the next section. Thus, as a consequence, new decision tools can be inserted as required just like old ones can be phased out. Finally, means for communication with other users at other nodes, among other things for exchange of information, information evaluation and decision making, must be available as well.

4.2 The risk-model

C^2-systems for preventive and operative management of crises must be based on models for determination and handling of risks, so called risk models. The resulting risk model incorporate the objects that should be protected, threats that are targeting those objects, the probability of those threats being realized, and the consequences it will have (Figure 4). In the model, existing threats relate to the objects. For each object and threat a risk determination is completed, based on the object's vulnerability, probability of the threat being realized and its consequences. The model also includes the capability to consider how preventive actions decrease the probability of a realization of the threat and the consequences. Hence, preventive actions can be performed to decrease an object's vulnerability and the consequences of a realization.

Consequences of a realization of a threat will not only have effects on the targeted object, but will generally also affect the objects environment. That is, an affected object is a threat against objects in its environment (e.g. fire in an oil storage), which in their turn, effected, could constitute threats against other objects. This chain reaction could be escalating as well declining. To decrease effects and prevent escalating chain reactions both operative and preventive actions could be performed.

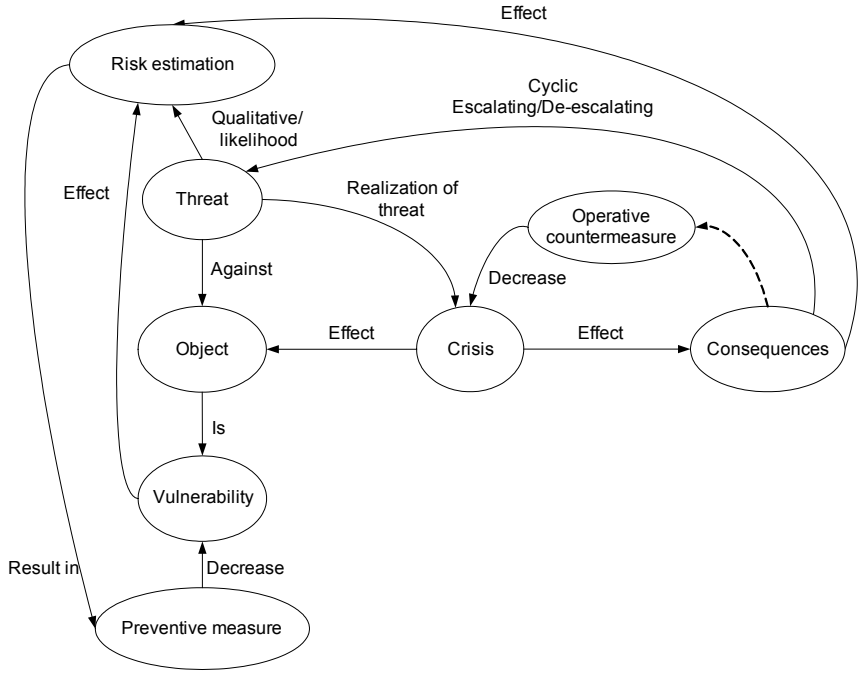

Figure 4. The risk model including its preventive and operative parts.

Experiences of consequences of real and simulated realizations of threats can be included in the risk model to make future risk determination more accurate. However, the risk model presented in this paper should be seen as initial step to develop a more complete risk model. A further developed risk model is possible to use as the foundation for simulation of threats, their consequences and possible chain reactions. The possibility to simulate and to make predictions will make it possible to take sufficient actions in both preventive and operative crises management.

5. SYSTEMS DEVELOPMENT FOR CRISIS MANAGEMENT

Systems development focuses on how to create new and/or change existing systems. In a broad sense, systems can be technical, organizational or combinations of these. To achieve systems that efficiently support intended operations, the technical and organizational parts of the systems have to be jointly developed in a harmonized way. Thus, a wide spectrum of competences has to cooperate.

The difficulty in developing, from the users perspective, the intended systems, on budget and on time have been acknowledged for some time, but the problems have so far not been entirely resolved [13], [14]. Main causes of these obstacles are in the lack of methodological support for system context modeling, elucidation of needs, transformation of those needs to requirements and to implement these requirements as systems features [15], [16].

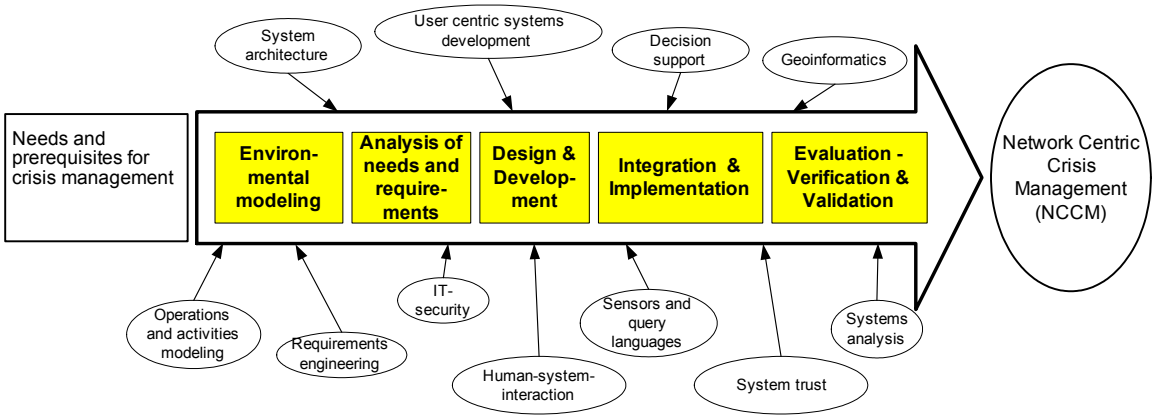

Figure 5. The relationship between the different research fields and the system development process.

A number of research areas have to be involved in the problem area of development of a command and control system for crisis management. In Figure 5 the different phases of a system development process is shown together with a set of possible concerned research areas.

5.1 Architectures

All systems have an architecture, independently of whether it is formalized or not. A formalized architecture can be used to describe and contemplate existing as well as future systems. Further, architectural approaches can be used for holistic and abstract description of complex systems. However, it could also be used for viewing of details in specific aspects of complex systems; the opposite to hide such aspects is not relevant for the moment.

System architecture approaches is beneficial in both development of new as well as modification and maintenance of existing systems, by providing rules for how components of a system should interact [17]. Thereby, it also makes it possible to reuse existing systems in combination with newly developed components, to achieve new functionalities and capabilities [18]. Hence, the use of architectural approaches makes it possible to have large and complex systems that are flexible and dynamic [19]. Hence, a well defined and used architecture is fundamental for network based organisations. It makes it possible to view the organization as a system-of-systems. It should also provide a foundation for how to construct information technology for communication and sharing information.

From the system architecture perspective crisis management can be viewed as a system. Hence, well formalized and feasible system architectures for crisis management can be used for development and maintenance. It would enhance the possibility to achieve organizations for crisis management that are dynamic and adaptive to the crisis environment, and that could make use of resources in the society. Resources that could when need be engaged in the work to prevent, handle, and decrease effects of crisis.

5.2 IT/information security

Future information systems will be extensive, ubiquitous and business/operation critical. To ensure the confidentiality, integrity and availability of the information handled by these systems as well as the systems themselves all aspects of security have to be thoroughly penetrated. As discussed in the introduction of this chapter, this requires an understanding of the system environment, which for example includes stakeholders and legal issues, and coordination between requirements engineering and IT security functions. This is a prerequisite for cost effective and efficient security solutions and, eventually, for achieving system trust.

To be able to reach these goals for systems supporting preventive and operative crisis management, design for securability is needed, that is, systems have to be designed in order to support the process of achieving a specified level of security in operation. Design for securability can be divided into three main processes:

- contextual modeling,
- security requirements engineering and
- security architecture design.

All three main processes are necessary during the entire life-cycle of a system and they are overlapping as well as interdependent. The purpose is that the design should be dynamic and evolutionary. The main processes contain several research issues requiring the invention of novel methods and techniques to enable a reasonable level of information and IT security. Central research issues are:

- Formulation of security related context modeling techniques and methods, possibly by extension of existing general context modeling approaches.
- Development of methods for security requirements engineering.
- Integration of these methods with corresponding methods for general requirements engineering, that is, the systems development process in large.
- Describing the relations between IT security level and trust.
- Specification of the relations between C^2, risk models, information, and IT security.

5.3 Decision support tools

Various types of decision support will play a central role in the command and control functionality based on the model discussed here. Among the required tools a relatively large part must be subject to further research to make it possible to solve some of the more important research issues. Several of the decision support tools that must be developed need, to a high degree, to be sufficiently general to be able to be used in several of the different applications. In many of the tools spatial/temporal information will be required, that is geo-information, but sensor data will have to be dealt with as well. As a consequence, a large number of methods for both data analysis and fusion need to be developed. Taken together this will clearly increase the complexity of the final system, including the requirements for a high degree of efficiency. Conclusively, the research efforts on this area must be highly comprehensive. Among the more important tools, of this kind, can techniques for query languages, data mining and higher order of information fusion, such as situation and impact analysis, be mentioned. Furthermore, most of the decision support tools must be able to interact with each other, e.g. geo-information must be used by the query language etc.

Finally, communication will play an important role in any activities carried out by the command and control model. This communication must take place on two levels. First between the end-users and secondly from the attached data sources and the users via the decision support tools. The latter type is obviously related to how to communicate the large data quantities generated by the data sources.

5.4 Human factors

Among the most important human factors research areas related to the design and evaluation of a C^2 - system for crisis management are information processing, decision making, and communication within and between teams at different levels of organisations within the command and control system. Important aspects of human behaviour are cognitive reasoning, sense-making, task-related performances and skills, mental and physical workload. Simulation, modelling, training and education are important when considering interface design and the operative use of the system.

In developing a system of systems it is necessary to engage and, in an optimized way, integrate knowledge about human abilities, valuations, reasoning and thinking in an early phase of the process to achieve a useful system. These ambitions not only lead to beneficial improvements of the system but also to economical savings. It is not enough for a system to be useful in only optimizing performance under reasonable workload. The system should also encourage and support emotional and motivational engagement and give people opportunity to be creative and trust the system in order to use them in the best possible way.

Early mission- and task analysis, iterative processes in the design including testing of performance and user evaluation of trust of the system must be regarded at all phases of the system development. International standards regarding the design process in system development connected to human needs and requirements should be regarded.

5.4.1 System trust

The trust in other people, authorities or a system in general involving both people and technical solutions is influenced by factors like predictability, dependability and faith. This means that the trust in e.g. a C^2-system is affected both by a history with the specific system as well as an idea or an expectation of how reliable the system will be in the future [20]. The trust in the system will also get different foundations depending on how far in the “familiarity-process" you have reached. From a rumour, via a vague acquaintance to a deeper knowledge and finally own experience in the system a basis for trust is developed. Apart from the sheer knowledge-based requirements, the resulting trust strongly contributes to how the system is used and best taken advantage of.

Thus, in a crisis situation, it is vital that the participants, both actors and exposed, have trust in each other and the crisis management system. People exposed to the crisis will probably feel great insecurity of what will happen to them, the vulnerability is obvious and the trust in the crisis management system that should handle the situation gets an essential and maybe crucial meaning [21]. This is, of course, also of vital importance for those who has to act to remove the crisis or mitigate its consequences.

From the discussion above, some groups in the society can be distinguished with different relations to and dependence on the crisis management system. On one hand those who are directly involved in the use of the system, the actors, and on the other hand those who, in some way, are exposed to the consequences of the crisis:

Actors;

- management (e.g. authorities, military, emergency services)
- performers (e.g. personnel in fire brigades, police, civilians)

exposed;

- directly (e.g. injured, related, organizational membership)
- indirectly (e.g. by identification, feeling of affinity)

Co-operation between actors and system is vital for synergic effects to occur. If the actors do not trust the system they will not fully use it or ignore it and only use their own judgements instead. A complex technical and social system like a C^2-system including an information network can not be expected to get immediate trust from the management or the performers, but they will need time and education to gain trust in these new tools.

For those who are considered exposed to the crisis, a feeling of nearness and affinity with the organization and system handling the crisis is of great importance for them to develop a trust in the crisis management

system. If they have trust in the actors, i.e. the management and the performers, the efforts in mitigating and removing the crisis are simplified.

Consequently, it is of outmost importance that everyone, both actors and exposed, have had the opportunity, under normal conditions, to get adequate knowledge in the crisis management system and a feeling of familiarity with the same. This way, they have, even in a crisis situation, better qualifications to have trust in the system and its abilities.

As trust is affected by the conception we have of the system already through rumours or a vague acquaintance, the marketing and implementation of a C^2-system is important if the system should receive the high and legitimate trust it deserves. It is also important that the system is not given a too high trust, a superstitious belief, as this also affects the co-operation with the system in a negative way.

5.4.2 Privacy

A C^2-system with a great need of information can cause extensive surveillance of the citizens in a community, which by many can be considered as a violation of their privacy. With a high understanding of the function of the C^2-system and its attentions, the requirements for a high trust is gained and thereby the feeling of violation of privacy should decrease or even disappear. Some aspects that can be of importance in increasing the understanding in the need for supervision by the C^2-system are that we:

- know who is performing the surveillance,
- sympathize with the surveillant,
- know the reason for surveillance,
- like or at least accept the reason for surveillance.

These aspects can be related to ideas connected to trust such as familiarity, intentionality, understanding and honesty. The problems in creating a high and legitimate trust in the C^2-system, seems to be close at hand when dealing with problems regarding privacy.

6. CONCLUSIONS

In this work, which still is at a preliminary stage, some architectural models for a command and control system have been discussed. The main application for the final command and control system will be concerned with crisis/emergency management. The proposed architectures center on a particular model for command and control. The structure of this model can basically be looked at as service oriented, that is a number of more or less complex decision support tools on fairly high level should be possible to integrate with the basic C^2-model, where each of these tools can be seen as particular services. Examples of such decision support tools are a query language for multiple sensor data sources, tools for data mining but also a GIS can be thought of. Each of these tools or services can subsequently allow allocation of other and more special services, for example, various types of sensors. Other aspect of concern in this work has been to consider such aspects as IT/Information security, system trust and HSI-techniques already at an early phase of the development of the C^2-system. For this reason, a specific technique for systems development for crisis management systems has been developed. The principles of this technique are also discussed in this paper. Besides, a module for risk analysis will also be integrated into the system. The purpose of the risk model is to accomplish analysis of risks that can be associated with various types of occurring objects that need to be protected with support from the C^2-system.

The C^2–system architecture that has been discussed in this paper will be subject to further studies in the near future.

REFERENCES

[1] Graser, T., Barber, K. S., Williams, B., Saghir, F., Henry, K. A., *Advanced consequence management program: challenges and recent real-world implementations*, Proceedings of the SPIE conference on Sensors and Command, Control, Communications and Intelligence (C^3I) Technologies for Homeland Defence and Law Enforcement, Orlando, FL, USA, April 1-5, 2002, pp 324-333.

[2] Rodrigues Nt, J.A.; Ulm de G. Lima, V.M.; Lima, G.M.P.S.; Ferreira, M.C.; Alves de Almeida, J.C.; de Oliveira e Cruz, S.; Cerqueira, R.F.G.; Martins, C.B., *A command and control support system using CORBA*, Proceedings 21st International Conference on Distributed Computing Systems, Mesa, AZ, USA, April 16-19, 2001, p 735-738.

[3] Modrick, J. A., *PRESTO: multi-media distributed network for collaborative work in command and control*, Proceedings of 40th Annual Meeting of the Human Factors and Ergonomics Society, Philadelphia, PA, USA, 1996, pp 758-761.

[4] Bammidi, P., Moore, K.L., *Emergency management systems: a systems approach,* 1994 IEEE International Conference on Systems, Man, and Cybernetics. Humans, Information and Technlogy, 2-5 Oct. 1994 , San Antonio, TX, USA , pt. 2, p 1565-70 vol. 2.

[5] Sutherland, J.W., *Model-base structures to support adaptive planning in command/control systems*, IEEE Transactions on Systems, Man and Cybernetics, vol. 20, no. 1, Jan.-Feb. 1990, p 18-32.

[6] Braim, S.P., Hepworth, N., *A fully-featured human computer interface for intelligence and command and control applications,* International Conference on Information-Decision-Action Systems in Complex Organisations (Conf. Publ. No.353), 6-8 April, 1992 , Oxford, UK, p 149-52.

[7] Wohlever, S., Fay-Wolfe, V.; Freedman, R.; Maurer, J., *Building adaptable real-time command and control systems using CORBA*, Fourth International Workshop on Object-Oriented Real-Time Dependable Systems, 27-29 Jan. 1999 , Santa Barbara, CA, USA, p 117-22.

[8] Worm, A., *On Control and Interaction in Complex Distributed Systems and Environments*, Linkoping Studies in Science and Technology, Dissertation No. 664, Linkoping University, Linkoping, Sweden, 2000.

[9] Hall, D.L., & Llinas, J. (Eds.)., *Handbook of Multisensor Data Fusion*, CRC Press, New York, 2001.

[10] Mena, J. *Investigative Data Mining for security and Criminal Detection,* Elsevier Science (USA), Burlington, MA, 2003.

[11] Erland Jungert et al., *From Sensors to Decision - Towards improved awareness in a network centric defence*, FOI-R--1041--SE, December 2003.

[12] Chang, S.-K., Costagliola, G., Jungert, E. and Orciuoli, F., *Querying Distributed Multimedia Databases and Data Sources for Sensor Data Fusion,* accepted for publication in the Journal of IEEE transaction on Multimedia, 2004.

[13] Brooks, F. P. Jr. (1995). The Mythical Man-Month: Essays on Software Engineering. Addison-Wesley.

[14] Chaos, The Standish Group, 1995, http://www.standishgroup.com/ (2004-02-27).

[15] Hallberg, N. (1999) *Incorporating User Values in the Design of Information Systems and Services in the Public Sector*, Linköping Studies in Science and Technology, Dissertation No. 596.

[16] Kotonya, G. & Sommerville, I. (1998) *Requirements Engineering. Processes and Techniques*, John Wiley & Sons, Wichester.

[17] Rechtin, E. (1999) S*ystems architecting of organizations: why eagles can´t swim*, CRC Press.

[18] Muller, J.K., (1995) Integrating architectural design into the development process. In *Proceedings of the 1995 International Symposium and Workshop on Systems Engineering of Computer Based Systems*, pp. 114 -121.

[19] Maier M. W. & Rechtin, E. (2002) *The art of systems architecting*. CRC Press.

[20] Thurén, R., J. Andersson, and M. Malm, *Systemtilltro*. 2003, FOI - Swedish Defense Research Agency: Linköping. p. 54 (In Swedish).

[21] Mishra, A.K., *Organizational responses to crisis: The centrality of trust*, in *Trust in organizations: Frontiers of theory and research*, R.M. Kramer and T.R. Tyler, Editors. 1996, Sage: Thousand Oaks, CA. p. 261-287.