Flexible role-handling in command and control systems

Examensarbete utfört i informationsteori

av

Fredrik Landberg

LITH-ISY-EX--06/3855--SE

Linköping 2006-12-04
Flexible role-handling in command and control systems
Examensarbete utfört i informationsteori
Vid Linköpings tekniska högskola
Av

Fredrik Landberg
LITH-ISY-EX--06/3855--SE

Handledare: Lars Westerdahl
Examinator: Viiveke Fåk
Linköping: 2006-12-04
Abstract
In organizations the permissions a member have is not decided by their person, but by their functions within the organization. This is also the approach taken within military command and control systems. Military operations are often characterized by frictions and uncontrollable factors. People being absent when needed are one such problem.

This thesis has examined how roles are handled in three Swedish command and control systems. The result is a model for handling vacant roles with the possibility, in some situations, to override ordinary rules.

Antal sidor: 52
Abstract

In organizations the permissions a member has is not decided by their person, but by their functions within the organization. This is also the approach taken within military command and control systems. Military operations are often characterized by frictions and uncontrollable factors. People being absent when needed are one such problem.

This thesis has examined how roles are handled in three Swedish command and control systems. The result is a model for handling vacant roles with the possibility, in some situations, to override ordinary rules.
Contents

1 INTRODUCTION ..................................................................................................................... 1
  1.1 Background ........................................................................................................................... 1
  1.2 Purpose .................................................................................................................................. 1
  1.3 Questions to be answered ...................................................................................................... 1
  1.4 Scope .................................................................................................................................... 2
  1.5 Method .................................................................................................................................. 2
    1.5.1 Validating the result ......................................................................................................... 3
    1.5.2 Method criticism .............................................................................................................. 3
  1.6 Structure ................................................................................................................................ 3

2 THEORY ..................................................................................................................................... 5
  2.1 Command and Control Systems .......................................................................................... 5
    2.1.1 Military history and philosophy ...................................................................................... 5
    2.1.2 Purpose of a command and control system ..................................................................... 7
    2.1.3 Environment .................................................................................................................... 8
    2.1.4 Network Centric Warfare ............................................................................................... 8
    2.1.5 Security in command and control system ....................................................................... 8
  2.2 Information security ............................................................................................................. 9
    2.2.1 Security basics .................................................................................................................. 10
    2.2.2 Access control ................................................................................................................. 11
    2.2.3 Security principles .......................................................................................................... 14
    2.2.4 Access Control Models ................................................................................................. 15
  2.3 Role Based Access Control .................................................................................................. 16
    2.3.1 Role ................................................................................................................................ 16
    2.3.2 RBAC definitions .......................................................................................................... 17
    2.3.3 RBAC framework ........................................................................................................... 17
    2.3.4 Delegation in RBAC ...................................................................................................... 18
  2.4 Governing documents ......................................................................................................... 19
    2.4.1 Governmental laws ............................................................................................................ 19
    2.4.2 Armed Forces regulations .............................................................................................. 20
    2.4.3 Swedish Armed Forces information security policy ....................................................... 20
    2.4.4 H SÅK IT 2006 ................................................................................................................. 21
  2.5 Related Work ....................................................................................................................... 22

3 COMMAND AND CONTROL SYSTEMS ................................................................................. 25
  3.1 Factors .................................................................................................................................. 25
  3.2 IS MARK ............................................................................................................................... 25
    3.2.1 Access control in IS MARK ............................................................................................ 26
    3.2.2 Role handling in IS MARK ............................................................................................ 26
  3.3 Swedish Command and Control Information System (SweCCIS) ......................................... 26
    3.3.1 Main functionality .......................................................................................................... 27
    3.3.2 Roles ............................................................................................................................... 28
    3.3.3 Security Requirement ..................................................................................................... 28
  3.4 Future system (FMLS 2010) ............................................................................................... 28
    3.4.1 Information security in FMLS 2010 ............................................................................. 30
    3.4.2 Role handling in FMLS 2010 ....................................................................................... 31
    3.4.3 Workgroup roles and permissions ............................................................................... 32

INTRODUCTION ..................................................................................................................... 1
  1.1 Background ........................................................................................................................... 1
  1.2 Purpose .................................................................................................................................. 1
  1.3 Questions to be answered ...................................................................................................... 1
  1.4 Scope .................................................................................................................................... 2
  1.5 Method .................................................................................................................................. 2
    1.5.1 Validating the result ......................................................................................................... 3
    1.5.2 Method criticism .............................................................................................................. 3
  1.6 Structure ................................................................................................................................ 3

2 THEORY ..................................................................................................................................... 5
  2.1 Command and Control Systems .......................................................................................... 5
    2.1.1 Military history and philosophy ...................................................................................... 5
    2.1.2 Purpose of a command and control system ..................................................................... 7
    2.1.3 Environment .................................................................................................................... 8
    2.1.4 Network Centric Warfare ............................................................................................... 8
    2.1.5 Security in command and control system ....................................................................... 8
  2.2 Information security ............................................................................................................. 9
    2.2.1 Security basics .................................................................................................................. 10
    2.2.2 Access control ................................................................................................................. 11
    2.2.3 Security principles .......................................................................................................... 14
    2.2.4 Access Control Models ................................................................................................. 15
  2.3 Role Based Access Control .................................................................................................. 16
    2.3.1 Role ................................................................................................................................ 16
    2.3.2 RBAC definitions .......................................................................................................... 17
    2.3.3 RBAC framework ........................................................................................................... 17
    2.3.4 Delegation in RBAC ...................................................................................................... 18
  2.4 Governing documents ......................................................................................................... 19
    2.4.1 Governmental laws ............................................................................................................ 19
    2.4.2 Armed Forces regulations .............................................................................................. 20
    2.4.3 Swedish Armed Forces information security policy ....................................................... 20
    2.4.4 H SÅK IT 2006 ................................................................................................................. 21
  2.5 Related Work ....................................................................................................................... 22

3 COMMAND AND CONTROL SYSTEMS ................................................................................. 25
  3.1 Factors .................................................................................................................................. 25
  3.2 IS MARK ............................................................................................................................... 25
    3.2.1 Access control in IS MARK ............................................................................................ 26
    3.2.2 Role handling in IS MARK ............................................................................................ 26
  3.3 Swedish Command and Control Information System (SweCCIS) ......................................... 26
    3.3.1 Main functionality .......................................................................................................... 27
    3.3.2 Roles ............................................................................................................................... 28
    3.3.3 Security Requirement ..................................................................................................... 28
  3.4 Future system (FMLS 2010) ............................................................................................... 28
    3.4.1 Information security in FMLS 2010 ............................................................................. 30
    3.4.2 Role handling in FMLS 2010 ....................................................................................... 31
    3.4.3 Workgroup roles and permissions ............................................................................... 32
APPENDIX 1. FÖRsvARSMAKTENS INFORMATIONSSÄKERHETSPOLICY.... 47

APPENDIX 2. THE INFORMATION SECURITY POLICY OF THE ARMED FORCES
.......................................................... 48

APPENDIX 3. SYSTEM OBJECTIVES.............................................. 49

BIBLIOGRAPHY .................................................................................. 50
Figures

Figure 1. Information security and its subparts ................................................................. 9
Figure 2. Relation between confidentiality, integrity and availability .......................... 11
Figure 3. Reference monitor mediating access ............................................................... 12
Figure 4. Access permissions using groups ................................................................. 13
Figure 5. Example of security level lattice ................................................................. 15
Figure 6. Access control permissions using RBAC ..................................................... 16
Figure 7. RBAC framework ...................................................................................... 18
Figure 8. Barka and Shandhu’s model of delegation .................................................. 19
Figure 9. Na and Cheon’s model for delegation ......................................................... 19
Figure 10. Security functions depending on information classification ..................... 22
Figure 11. SWECCIS design structure ...................................................................... 27
Figure 12. Normal role relations ................................................................................. 33
Figure 13. Model relations ......................................................................................... 34
1 Introduction

Information about the battlefield is so important that armed forces spend a lot of money each year to develop command and control systems.

Command and control system – The facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned and attached forces pursuant to the missions assigned. (US DOD dictionary, 2001)

These compile information from a wide array of sources to support the commander’s decision taking. The change on to a digital medium could make the structure less flexible. Before digitalization, if someone did not show up or was missing in action, anyone could step up and fill their place. In the digital domain there are strict boundaries on what actions one person can and cannot do, mainly because of security precautions. The downside is you might not be able to access the information you need, because you do not have the rights to do so.

1.1 Background

In a command and control system there are high demands on confidentiality and integrity. This is reasonable because the gathered information could, in the hands of the enemy, make us vulnerable. A command and control system would also be pointless if the information could not be trusted because of integrity violations. Compiled but uncertain or unreliable information does not support the commander in making sound decisions.

Normally permissions to perform actions within a command and control system are based on roles. The rights are not connected to a physical person, but to the roles they perform. Still, the physical person is responsible for the actions they commit when acting in their role. Thus it must be possible to trace which person that has been acting in which role during which time period.

One potential problem is vacant roles, since actions or information is only accessible to the holder of a specific role. Because a command and control system operates in a highly dynamic environment, vacant roles are likely to occur. If this happens there must be a policy how to appoint the vacant role to someone else to avoid information falling between chairs.

1.2 Purpose

The purpose of this thesis is to examine the methods and technical implementation used in command and control systems to appoint roles to physical persons. The aim is to try to create a model which enables users to extend their rights and to be able to solve their mission without making too large a sacrifice on security issues.

1.3 Questions to be answered

- How and under which circumstances can users of a command and control systems temporary extend their rights (enter another role) to be able to complete their mission without sacrificing security?
  - Are vacant roles a large problem in command and control systems?
    - How is this solved in existing and future command and control systems?
  - Which criteria could be used to decide if a user should be allowed to acquire a role which they have not been predefined for?
How could those criteria be designed to avoid wrongful incremental of rights?
What will impede users from exceeding their authority, consciously or unconsciously?
  o What would a model that implements this look like?
  o Is the resulting model better than existing solutions?

1.4 Scope
There are a number of assumptions made to narrow the scope of this report.

- The thesis mainly treats Swedish tactical and operational systems, and is adopted to follow Swedish laws and regulations.
- The command and control system is regarded as one single system with one policy applied to it.
- Roles are used and there is a well established organizational structure that is commonly known to the user of the system.
- The information and services that are provided by the command and control system are presumed to be classified into categories and connected to appropriate roles.

1.5 Method
The work was started by a brainstorming with the purpose of finding different approaches to the subject. The result was used to create the questions to be answered, the scope of the report and a draft of the system objectives. The system objectives were then used as a guideline during the work to evaluate the found information and to evaluate the existing systems. The system objectives are included in appendix 3.

The theoretical part of the thesis gives background knowledge and summarizes the different areas treated. It also defines the terms that are used later on in the thesis. Then the search for information and research papers on these subjects begun. The focus was on recent articles and papers that are related to the questions to be answered and the model objectives. The information found was used to refine and revise the questions to be answered and the model objectives.

In the study of existing systems, informal interviews with people participating in the work of developing command and control systems were made. The systems documentation was also examined to see how the roles were implemented in those systems. The information found was used to create a picture of existing command and control systems, and to furthermore revise the model objectives.

Based on the theoretical part and the information gathered when studying the existing systems, a model was proposed to handle roles in a more flexible way than the existing ones do. By flexible it means a way to circumvent the normal rules when availability is a more important issue than confidentiality and integrity, without forgoing the demands on security on the whole. Finally the model was compared with the other systems.

The next natural step would be an implementation to be able to compare the system side by side to an existing one, but that falls outside of the scope of this work, because of the limited timeframe and the lack of available systems to compare to.
1.5.1 Validating the result
To be able to show if the model is a better approach than an existing system, the results will be validated by comparing the existing system and the proposed model. As a guideline the model objectives was used, which can be found in appendix 3.

1.5.2 Method criticism
When comparing a real system with a model, there is always a risk of unconsciously changing the fact as it suits the author view of the world. The risk of doing so is indeed greater if one of the proposed theories is invented by the author. As Zelkowitz and Wallace (1998) points out in their article Experimental Models for Validating Technology, the author of this thesis is both the subject and the leader of the experiment. They call this way of evaluating a system assertion. They stress that there is a possibility of biased result when using assertion. To avoid biased results the model objectives were created beforehand stating requirements on the system. And the list of objectives is then used in the evaluation. The result should therefore be fair.

1.6 Structure
The report is presented to the reader in a rather straightforward way. The report could be read straight through or in parts depending on the reader’s level of expertise and interest.

Section 1 Presents the subject, task, purpose and method used in this report.

Section 2 Presents the fundamental parts that are needed to understand the rest of the report. It defines expressions used in the report. It also gives a more in depth explanation of the nature of the problem. This part also contains related work.

Section 3 The three examined systems are described.

Section 4 It describes the model that is constructed by information and facts gathered in the previous two sections.

Section 5 This section can be regarded as the result of the thesis, where the existing system is compared to the model. There is also a validation part where the result is analyzed to see if the result is useful.
2 Theory

Command and control systems have their foundation in the doctrines used which in turn rely on experience through history. This section will give the reader a summary of the background and purpose of command and control systems. It will also explain the area of information security and the expressions that need to be defined. Also, the rules and legislation comprising military command and control systems will be treated. Finally, related work in the area of flexible access control solutions is presented.

2.1 Command and Control Systems

Every conflict is a struggle of peoples' will. The dynamics in human action together with the complexity of war and unforeseen events generates uncertainty. The uncertainty can be reduced by gathering information. Absolute security is precluded by the nature of battle. The gist of military command is the coordination of human action and resources in complex and dynamic situations, often in uncertainty and in lack of time. (Freely translated)

Varje konflikt är i grunden en kamp mellan människors viljor. Dynamiken i mänskligt agerande, tillsammans med krigföringens komplexitet och förutsedda händelser, genererar osäkerhet. Osäkerheten kan minska, bland annat genom informationsinhämtning. Absolut säkerhet omöjliggörs emellertid av stridens natur. Kärnan i militär ledning utgörs av samordning av mänskligt agerande och resurser av olika slag i komplexa, dynamiska situationer, ofta under stor osäkerhet och tidspress. (Försvarsmakten [1])

To help the commander to decrease the level of uncertainty and facilitate coordination, technology can be used. Command and control system (swe. ledningssystem) does not necessarily involve computers and digital networks, it could be operated by any means of communication. In some contexts it is not even a purely technical system but an entirety of method, technology, organization, and personal abilities (Försvarsmakten [3]). The definition used by the US Department of Defense (DoD) is:

Command and control system – The facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned and attached forces pursuant to the missions assigned. (US DOD dictionary, 2001)

The term command and control system is also used to describe the technical system, used by organizations to make and effectuate decisions. In some contexts this is named command and control support system (swe. ledningsstödssystem). In this thesis the term command and control system is used to describe the technical system.

2.1.1 Military history and philosophy

To explain why a command and control system is needed and some philosophies that have influenced military behavior, a journey back in time is needed. The journey starts as early as 600 BC with three quotes from Sun Tzu, a Chinese general.
If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

Maybe Sun Tzu intended this in a psychological way, but to be successful in war or in other complex and dynamic situations the commander needs to be aware of what happens on the battlefield and take appropriate actions. Sun Tzu also said

The spot where we intend to fight must not be made known; for then the enemy will have to prepare against a possible attack at several different points; and his forces being thus distributed in many directions, the numbers we shall have to face at any given point will be proportionately few.

This quote shows the importance of secrecy and deception in war was known a long time ago and that the information about the battlefield is valuable.

To fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting.

The last quote from Sun Tzu enables a giant leap in time to the early 20th century, when an expression for what Sun Tzu said was introduced by Liddell Hart. The expression was indirect approach. It was a reaction to the First World War, which could be described as a typical example of a direct approach, where the main forces met head on. Hart came up with the expression when studying old battles. Hart meant that by avoiding the main forces and striking against weaker but important parts of the enemy, the war could be won without heavy casualties. (Rekkedal 2003)

Hart expressed himself like this.

Dislocation of the enemy’s psychological and physical balance has been the vital prelude to a successful attempt at his overthrow. This dislocation has been produced by a strategic indirect approach. (Hart 1965)

This quote is the gist of what later became known as maneuver warfare which is the dominating doctrine used by western countries in the latter part of the 20th century. Getting the enemy off balance is a good metaphor, because just like a boxer cannot deliver a forceful punch when he is out of balance, an army out of physical or psychological balance cannot do as much damage. This was picked up by US Air force colonel John Boyd, when he watched the outcome of the air to air fights during the Korean War, where the Russian built airplane was technologically superior to the American in many aspects. But the American planes had better visibility from the cockpit. The Americans used this advantage of being able to react and orient quicker and they were very successful. Boyd then created a model named the OODA-loop, which is an abbreviation for observation, orientation, decision and action. He asserted that the organization that could execute the decision loop quickest and continuing being faster than the opponent would eventually bring the opponent off balance. And thus be able to defeat the same. (Rekkedal 2003)

The OODA-loop stresses the importance of maintaining initiative, just as in chess or even tic-tac-toe. If you lose the initiative you will be forced to react rather than act, and this could be difficult to recover from. It is therefore a golden rule in the Swedish Army that:
Irresoluteness and lack of power to act will often have more serious consequences than mistakes in the course of action. (Freely Translated)

Obeslutsamhet och bristande handlingskraft får oftast allvarligare följer än misstag i fråga om tillvägagångssätt. (Försvarsmakten [2])

The key in the statement is that it is more important to do something, than stalling while deciding which would be the optimal method of operation. This is because war, unlike tic-tac-toe or chess, has more uncertainty built in and as Helmuth von Moltke said:

No plan of operations extends with certainty beyond the first encounter with the enemy’s main strength

This takes us to the next expression that needs to be explained; Mission type tactics or Directive control (Auftragstaktik in German, uppdragstaktik in Swedish). This became commonly known after the Second World War, but can be traced back to the early 19th century (Rekkedal 2003). There are different opinions on the definition of directive control; the Swedish version is presented here:

Directive control is performed by a commander, which gives a mission, guidelines and allots resources but lets the person, to the greatest extent; decide how the mission should be solved.

Uppdragstaktik utövas genom att chef ställer uppgift, ger riktlinjer och tilldelar resurser samt låter den som löser uppgiften i största möjliga utsträckning själv bestämma hur den skall lösas. (Försvarsmakten [2])

This means that Directive control is a way of leading. It is performed by issuing a task, give guidelines and allot resources. But the way the task is solved is decided by the person in charge of that task. This gives the subordinate a possibility to act in accordance with the commander’s intent. Therefore subordinates can take initiative on their own and explore opportunities as they arise during execution of the task. (Rekkedal, 2003) This gives a higher degree of flexibility and a possibility to keep up pace to get the enemy off balance. This also provides the capability to continue an operation even if commanders are unavailable or communications brake down. (Försvarsmakten [3])

2.1.2 Purpose of a command and control system.

By using the information and services provided by a command and control system the commander can achieve battle space awareness (Swe. Behovsanpassad situationsuppfattning). Battle space awareness is the ability to see all the factors that affects the situation or maybe what Sun Tzu meant by “knowing the enemy”.

**battle space awareness** – Knowledge and understanding of the operational areas’ environment, factors, and conditions, to include the status of friendly and adversary forces, neutrals and noncombatants, weather and terrain, that enables timely, relevant, comprehensive, and accurate assessments, in order to

---

2 Armé reglemente del 2 (AR2)
3 Armé reglemente del 2 (AR2)
4 Grundsyn Ledning
successfully apply combat power, protect the force, and/or complete the mission. (US DOD dictionary, 2001)

One way to increase battle space awareness is to create an operation picture. By visualizing the battlefield it gives the commander a foundation for his decisions. Operational picture has been used for a long time. What a command and control system could give you is a common operational picture. A common operational picture is a shared view of the battle field, looking the same for all users. This together with the enhanced possibilities to communicate enables coordination between units. By this synergy effects can be achieved, which means that the sum of the combined effort is greater than the sum of the individual parts. This in turn leads us to the main purpose of a command and control system: To be able to utilize the resources at hand in the best possible way.

The use of a common operational picture may result in decision superiority (Swe. Ledningsöverläge). The concept decision superiority is used to describe the situation where the own organization observes, orients, decides and acts in a more successful way than the opponent. (Försvarsmakten [4])

2.1.3 Environment
The command post is one central point where a command and control system is used. A command post is an organizational unit in which people in cooperation use common methodology and an adopted technical support system. The command post’s location is decided on the basis of the mission. This could be inside as well as outside the area of operation and in one location or distributed in the area. The environment in which a command post is located is often demanding. The situation is often complex and chaotic and misunderstandings could result in large consequences. (Stenius 2006)

In an environment like this frictions are unavoidable, people will not show up on time, communications will fail and all sorts of minor events will occur. The important thing is the ability to handle these events.

2.1.4 Network Centric Warfare
Network Centric Warfare, NCW (Swe. Nätverksbaserat Försvar, NBF) is a concept with both visionary and doctrinal elements. It emerged in different studies in latter years of the twentieth century. NCW means that the abilities of the individual parts within the organization are made available for common use. This should create new abilities by combining others and increase the level of flexibility by combining the requested abilities to fulfill a certain mission. (Försvarsmaken [1])

It has been decided by the Swedish Government that the future development of the Swedish Armed Forces should be based on the ideas of NCW. (Ibid)

2.1.5 Security in command and control system
If information is disclosed to the enemy, they might know your plans and could prepare for them. If the information you have cannot be trusted, it is not used and is therefore worthless. Finally, if the information is not available when needed, it is also useless. This stresses the need for information security within a command and control system.

---

5 Militärstrategisk doktrin
6 Ledsvyst mål och riktlinjer
2.2 Information security

Information security is about protecting information in which ever form it is stored. Information security could be divided into a number of sub-categories. It consists of administrative security which includes methodology and routines used to enforce security. The other part is technical security, which includes the mechanisms used to enforce security. This in turn consists of physical security which is the physical protection of the information or location where the information is stored. The other part of technical security is computer security. See Figure 1 for an overview. In some contexts computer security is divided further but that is not of importance here.

![Figure 1. Information security and its subparts](image)

It is important to understand that information is an asset; it has a value and needs to be protected. When trying to protect the assets there are three different categories of protective measurements.

- Prevention: take measures to prevent your assets from being damaged or disclosed
- Detection: take measures that allow you to detect when an asset has been damaged, how it has been damaged and who caused the damage.
- Reaction: take measures that allow you to recover your assets from damage.

To be able to control what assets that needs protection and how, a security policy is needed. A security policy is the first of the fundamental requirements in the DoD TCSEC (The Orange book) for secure systems. (US DoD 1985).

Security Policy – The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. (US DoD 1985)

A security policy is a statement of what is, and what is not, allowed (Bishop 2005)

When the policy is settled, it needs to be enforced. This is done by implementing security mechanisms. One thing that should be noted is that a security mechanism is not necessarily a technical mechanism; it could also be organizational or procedural.

A security mechanism is a method, tool, or procedure for enforcing a security policy. (Bishop 2005)

This thesis will mainly discuss the technical mechanisms, i.e. computer security. Finding a definition of computer security is easy, but they all seem different. Here are some examples.
Computer Security – The protection of information assets through the use of technology, processes, and training. (Microsoft 2006)

Computer security deals with the prevention and detection of unauthorized actions by users of computer systems. (Gollmann 1999)

Computer Security – The means that aim to achieve and maintain the level of security that is brought upon an IT-system by laws, regulations, Armed forces statues, Armed forces information security policy, special written communication and the demands of current activity. (Freely translated)

Åtgärder som syftar till att uppnå och vidmakthålla den nivå av säkerhet som bl a lagar, förordningar, Försvarsmaktens författningar, Försvarsmaktens informationssäkerhetspolicy, särskilda skrivelser och verksamhetens behov ställer på ett IT-system. (Försvarsmakten [5])7

We can conclude from these that computer security is about protecting things of value within a technical system (Gollmann 1999)

2.2.1 Security basics

The ways in which the information can be compromised and protected, can be divided into three categories.

- **Confidentiality**, to prevent unauthorized disclosure of information.
- **Integrity**, to prevent unauthorized or erroneous changes to the information.
- **Availability**, to make sure the information is available to authorized requests without delay.

Confidentiality is about secrecy; the information should be accessible only to those authorized. A breach of confidentiality could for instance reveal your battle plan with fateful consequences.

Integrity issues could affect in multiple ways. If the information is maliciously modified, it could cause more disastrous decisions than if it would have been correct or even if the information was not available at all. The other way is if numerous errors are encountered within the information. Then the trust in the system might be lost and the system will not be used.

Data Integrity - The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction. (US DOD 1985)

Availability concerns that information should be available when needed. If the information about the enemy approaching you comes after the attack begun, it is already too late.

The problem is that these factors counteract each other and you cannot have them all at the same time. For instance a high level of confidentiality would degrade the availability and vice versa. An example is if you implement a very high degree of confidentiality by using cryptology you will have less degree of availability. But if everyone is allowed to access and

7 H SÄK IT
edit the data, availability is high, but confidentiality and the integrity are low. This could be illustrated by a triangle with the different categories in the corners and an area in which your system belongs, see Figure 2.

![Figure 2. Relation between confidentiality, integrity and availability.](image)

If all areas cannot be protected at the same time and by this fail to prevent wrongful actions, the next best thing to do is to be able to trace the responsible for the wrongful actions committed in the system. This requirement is called, Accountability. Accountability is the possibility to trace actions back to an individual. This is done by logging all important activities which creates an Audit Trail.

*Audit Trail - A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, and/or backwards from records and reports to their component source transactions. (US DoD 1985)*

There is also a stricter version of accountability, which is called non-repudiation. Non-repudiation means that a person cannot deny that the person has committed a certain action. One example of this is digital signing of documents.

### 2.2.2 Access control

To be able to distinguish which information that should be available to whom and who is allowed to change which data, an access control system is needed. But first some expressions need to be defined.

A subject executes an access operation to an object. The subject is the active part of the event; it could be a user or a process. What the subject does is called an access operation, it could be for example reading, modifying or deleting. The object is the passive part of the event; this is the resources of the system, typically a file or a service. The three parts together (subject, action, object) is called a permission triplet or privilege. In some circumstances there are also transactions. A transaction is a well defined method that could be used to modify data in an appropriate way.

*Object – A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of*
objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes, etc. (US DoD 1985)

Subject - An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. Technically, a process/domain pair. (US DoD 1985)

The access control system has a set of rules defined regarding which subject could do what access operations to which object. The rules could be defined as an access control matrix; this is a rather self-explanatory model where the matrix is made up by rows according to the subjects and columns according to the objects. In the crossing of the two the allowed access operations are written, see Table 1.

<table>
<thead>
<tr>
<th>Alice_diary.txt</th>
<th>Notepad.exe</th>
<th>Bob.html</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>{read, write}</td>
<td>{execute}</td>
</tr>
<tr>
<td>Bob</td>
<td>-</td>
<td>{execute}</td>
</tr>
</tbody>
</table>

Table 1. Access matrix

But in real systems this is often not a workable solution, due to the size of the matrix, so either capabilities or access control lists (ACL) is used. The difference between the two is where the allowed access operations are stored. In the capabilities model the access operation is stored together with the subject. For example, Bob would have a list containing the information that he is allowed to execute notepad.exe and read and write the file bob.html. The other way is to store the access rights with the object. The access control list for the file bob.html would contain, Alice: {Read}, Bob: {Read, write}.

The normal approach when a subject wants to perform an access operation to an object, is that the subject requests to do the desired action to something called a reference monitor. The Reference monitor then checks if it is allowed, and grants or denies access based on the applied set of rules. If the request is allowed, the reference monitor gives the subject the possibility to access the specified object. The decision made by the reference monitor is called an authorization. All accesses to objects should be mediated by the reference monitor, see Figure 3.

Figure 3. Reference monitor mediating access

A more formal definition of a reference monitor taken from TCSEC.

Reference Monitor Concept - An access control concept that refers to an abstract machine that mediates all accesses to objects by subjects. (US DoD 1985)
Authentication
The subjects also need to be connected with users, processes or systems. This is done through authentication. Authentication is to tell the system who you are, then use something to verify this. Authentication can be based on one or more of the following factors.

- Something you know, such as a password.
- Something you have, such as a smartcard or key.
- Something you are, such as fingerprint or retinal pattern.

Using more than one of the above factors at the same time is called strong authentication.

Authenticate - To establish the validity of a claimed identity. (US DoD 1985)

Groups
When administrating access control, using individual permissions between each subject and object would soon be impossible to handle. Therefore there is often the notion of groups. A group is a logical unit to which subjects or objects could be added. Then the group is assigned capabilities or the group is included in ACL’s. In this way you could more easily set up appropriate rules. For example all users in a system could be member of the group user and all the printers could be members of the printers group. Then only one rule is needed to enable all users of the system to print their documents at any available printer instead of one rule per printer-user pair. In a system with 9 users and 3 printers the none-grouped method would demand 27 rules. The usage of groups does not exclude the possibility to create relations directly between users and permissions, as could be seen in Figure 4.

![Figure 4. Access permissions using groups](image)

Access control system types
In access control systems there are some basic types of systems. One of them is discretionary access control, (DAC). In DAC the owner of the object chooses which subject that should be able to access it.

DAC – A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) onto any other subject (unless restrained by mandatory access control). (US DoD 1985)

In Mandatory Access Control (MAC), the rules cannot be altered by the individual user, and the authentication is performed by a system mechanism.

MAC – A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the object and the formal
authorization (i.e. clearance) of subjects to information of such sensitivity. (US DoD, 1985)

In originator controlled access control (ORCON or ORGCON) the creator of the object, not the owner, decides who gets access to the object.

All of these could be used alone, but in many cases the access control system is a mixture of them.

### 2.2.3 Security principles

In time a number of different security principles have evolved to help organizations with their security work. The principles below are a summary from Matt Bishop’s (2004) book, if not stated otherwise, *Introduction to computer security*.

The principle of **least privilege** is a principle used to avoid accidental or intentional abuse of the system. It states a subject should only have those permissions necessary to perform their task.

**Principle of least privilege** – This principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use. (US DoD 1985)

The principle of **fail-safe defaults** states that unless a subject is given explicit access to an object, it should be denied access.

The principle of **Economy of mechanism** states that a security mechanism should be as simple as possible. This principle also has another name, the **Principle of simplicity**. A simple system is easier to supervise and less prone to errors.

The principle of **complete mediation** states, that all accesses to objects are checked against the rules, even if the object has been accessed before by the subject.

**Separation of duties** specifies that every critical function needs to be approved by two separate subjects before it is carried out. One example could be that one person cannot sign the invoice of orders laid by him to prevent embezzlement.

Separation of duties could be either static or dynamic. In static separation of duties you organize the roles so that no one can ever occupy both the roles required to commit a transaction that is supposed to be protected by separation of duties. In organizations where persons could have multiple roles there is the need to check so one user does not occupy both roles needed to commit a protected transaction at the same time. (Ferraiolo et al, 2003)

**Separation of duties** – Dividing responsibility for sensitive information so that no individual acting alone can compromise the security of the data processing system. (ANSI 2000)

The principle of **Psychological acceptability** states, that the security system should not make the resource harder to access than if the system were not present.
2.2.4 Access Control Models

The military was one of the first computer users that demanded security. Their main concern was unauthorized disclosure of secret information. In 1973 David E. Bell and Leonard La Padula wrote a report on computer security where they introduced a model that could mathematically prove if an access control system was secure or not. Their focus was to hinder subjects on lower levels to access information on higher levels. The levels could be a representation of the classification security levels, such as RESTRICTED, CONFIDENTIAL, SECRET, and TOP-SECRET. This model demanded that no subject could read at a higher level (more secret) than the one it belongs to and not write to any level below its own. The first rule is rather self explanatory. The other one is there to prevent, intentionally or unintentionally, flow of classified information down through the levels and because of this become accessible by a subject without the proper security clearance. (Bell & La Padula 1976)

Biba presented another model that instead of focusing on unauthorized disclosure, focused on integrity preservation. In the Bell La Padula model anyone could write or modify TOP-SECRET messages or even delete them because everyone has clearance to write to higher security levels. The Biba-model works in the same way as Bell La Padula, but you are only able to read information with higher or the same integrity level as yourself and only write to the same and lower levels. The model ensures that no invalid information could be inserted into higher levels. If information from lower levels after all needs to be transferred to a higher level, this should be done by a certain function that checks the information before the transfer. (Biba 1977)

The two models above are described in a linearly ordered hierarchy, but this could be extended by dividing information into categories. A subset of categories is called a compartment. This is then used to create a partial order of the categories. If a subject for instance wants to access information belong to one security level and one compartment. Then the subject needs to be classified for at least the security level of the object and belong to all categories of the compartment. The partial ordered model is called a security lattice and an example can be seen in Figure 5. (Sandhu 1993)

![Security Level Lattice](image_url)

**Figure 5. Example of security level lattice**

In 1987 David Clark and David Wilson presented another model that focused on how to preserve information integrity. Commercial companies were more interested in preserving the
integrity of their information to prevent fraud or errors. So their model is based on the principle of separation of duties and the principle of well-formed transaction. The principle of well-formed transactions states that a subject cannot manipulate data arbitrarily but only in constrained ways that preserves the integrity of the data. This means that the only way to modify data is to use approved programs or methods. These are called transactions. For example maybe all changes of data need to be logged, and all transactions that modify data also write to a log. (Clark & Wilson 1987)

2.3 Role Based Access Control

The need for information within an organization often depends on the person’s job function. This is why job function often decides which permissions the person should have to access that information. Conventional access control methods are hard to implement in an easy administrative way. (Ferraiolo et al. 2003)

Using DAC is a problem because the employees do not own the information they have access to or have created, it belongs to the organization. The user is therefore not always allowed to make decisions about who shall have access to the information. (Ibid)

MAC was originally created to preserve confidentiality, which is not always the main concern of ordinary enterprises. (Ibid)

In 1992 Ferraiolo and Kuhn proposed a solution to this, which they called Role Based Access Control (RBAC). It is an abstraction layer in between the user (subjects) and the objects, almost like a group, but without the possibility to connect individual permission between subjects and objects. The abstraction layer is the role, were a role is a semantic construction around which an access policy is formulated. Permissions are authorized for roles and roles are authenticated for users in many-to-many relations, see Figure 6. (Ibid)

![Figure 6. Access control permissions using RBAC](image)

RBAC has proved itself to be a good solution for many organizations. It has several benefits over traditional MAC and DAC because it provides more flexibility and detailed control. It is also an effective way to handle personnel changes. When someone changes job positions the only thing that needs to be changed is the user-to-role relation. (Ibid)

2.3.1 Role

The role as seen here is an abstraction layer around which the access policy is formulated. It is also important to see how the real world relates to roles. In a well structured organization with well established routines one user could probably carry out his tasks by only using one single role. In more complex organizations it could be better to have a number of basic roles which are then combined to fit a job position. This means that one user could use several roles at the same time.
2.3.2 RBAC definitions

The solution is based on three rules: (Ferraiolo et al, 2003)

1. **Role assignment:** A subject can execute a transaction only if the subject has selected, or been assigned to, a role. The identification and authentication process (e.g. login) is not considered a transaction. All other user activities on the system are conducted through transactions. Thus, all active users are required to have some role.

2. **Role authorization:** A subject’s active role must be authorized for the subject. With rule 1, this rule ensures that users can take on only roles which they are authorized to.

3. **Transaction authorization:** A subject can execute a transaction only if the transaction is authorized for the subject’s active role. In concert with rule 1 and 2, this rule ensures that users can execute only transactions for which they are authorized.

This could be formulated in a more formal way: (Ferraiolo & Kuhn, 1992)

For each subject, the active role is the one that the subject is currently using:

\[ AR(s:subject) = \{\text{the active role for subject } s\} \]

Each subject may be authorized to perform one or more roles:

\[ RA(s:subject) = \{\text{authorizes roles for subject } s\} \]

Each role may be authorized to perform one or more transactions:

\[ TA(\{r:role\}) = \{\text{transactions authorized for role } r\} \]

Subjects may execute transactions. The predicate \( exec(s, t) \) is true if subject \( s \) can execute transaction \( t \) at the current time, otherwise it is false:

\[ Exec(s:subject, t:trans) = \text{true iff subject } s \text{ can execute transaction } t. \]

1. \( \forall s : subject, t : tran (exec(s, t) \Rightarrow AR(s) \neq \emptyset) \)
2. \( \forall s : subject (AR(s) \subseteq RA(s)) \)
3. \( \forall s : subject, t : tran (exec(s, t) \Rightarrow t \in TA(AR(s))) \)

The observant reader notices that this model does not take the object into consideration when deciding if an operation is allowed or not. To implement this a fourth rule is needed.

\[ \forall s : subject, t : tran, o : object (exec(s, t) \Rightarrow access(AR(s), t, o)) \]

2.3.3 RBAC framework

When the notion of RBAC emerged in the early 1990’s it was recognized for its usefulness, but there was little agreement on what RBAC meant. To settle this, a framework of four reference models was presented. (Sandhu et al, 1996)

The basic version with the three main rules was called RBAC0. It represents the minimum requirement for a role based authentication systems. But this had evolved and other functionality had been added. Since one natural way of structuring job functions in an organization is in a hierarchical way, RBAC1 has included functions to reflect the lines of authority and responsibility. This means that roles could inherit permissions from other roles, so that for instance a physician can inherit the permissions of a health-care provider if a physician is senior to the health-care provider. (ibid)

RBAC2 is another advanced model which uses the RBAC0 as a base and expands it by adding constraints, like for instance separation of duties. It is also possible to model a constraint in such a way that it would subdue hierarchies. (ibid)
Finally RBAC3 includes the features of the other three models, see Figure 7.

![RBAC framework](image)

Figure 7. RBAC framework

### 2.3.4 Delegation in RBAC

The basic idea behind delegation is that some active entity in a system delegates authority to another entity to carry out some functions on behalf of the former. (Barka & Shandhu 2000)

In an organization superiors often have permission to perform actions not allowable to subordinates. When a superior is absent, the organization cannot accept interruptions of normal activities. This requires the use of delegation, where a subordinate gets temporary permission to carry out the superior’s duties.

Barka and Shandhu’s paper *framework for role-based delegation models* from 2000 presents a model of how human to human delegation could be modeled using RBAC. They present a number of different use-cases that could be used for formalizing aspects of delegation. These use-cases identified a number of characteristics of delegation, which include:

- **Permanence** – If the delegation is temporary or permanent.
- **Monotonicity** – Refers to what powers the delegating role has after delegating. Monotonic means that the person still have the abilities left after delegating, or non-monotonic where the role loses its abilities when delegating.
- **Totality** – If the delegation is total or partial. Total delegation means to delegate all permissions and partial to only delegate a subset of the permissions.
- **Administration** – The term describes how the delegation is initiated. There are two types of delegation: self-acted and agent-acted delegation. Self-acted delegation is common and means that someone delegates a role occupied by themselves. Agent-acted delegation is when a trusted third party delegates the role on behalf of the original user. This could be useful in the case where the delegating role is not available. It is not allowed for the agent to delegate a role to him or her self
- **Levels of delegation** – If it should be allowed to further delegate a delegated role?
- **Multiple delegations** – If it should be possible to delegate a role to several others at the same time?
- **Agreements** – It could be bilateral or unilateral agreements in a delegation. In bilateral agreements both the delegating role member and the delegated member agree to delegate the role. In unilateral agreements the delegating member decides who shall be allotted the role independently if the delegated member agrees to this or not.
• **Revocation** – Revocation is the ability to recall the delegation and thereby remove privileges from the delegated member.

![Barka and Shandhu’s model of delegation](image)

**Figure 8. Barka and Shandhu’s model of delegation**

These characteristics are then incorporated into a structure which could be seen in Figure 8. This should show the useful combinations of the different characteristics. It is not complete with all combinations because the intent was to reduce the number of combinations to only include plausible and useful combinations. (Barka & Shandhu 2000)

SangYeob Na and ShuHyun Cheon presented in 2000 a model for delegation within RBAC using hierarchies. They presented a delegation server which could handle requests for delegation according to their protocol. The grantor sends a delegation request (1) to the delegation server and the server make a decision and sends a request result (2) back to the granter. It also sends a delegated role information message (3) to the grantee which includes the permission to perform the delegated actions, see Figure 9.

![Na and Cheon’s model for delegation](image)

**Figure 9. Na and Cheon’s model for delegation**

### 2.4 Governing documents

There are numerous documents specifying requirements on a command and control system. In this thesis Swedish legislation and regulations are used. It should not be hard to translate this to other countries’ condition, at least since Swedish Armed Forces changed their security classification levels to match the ones used within NATO and the US Armed Forces.

#### 2.4.1 Governmental laws

The main laws that affect the security aspects when a command and control system is constructed, is the law regulating the handling of classified information. In Swedish
legislation this is regulated by the Säkerhetsskyddslagen (1996:627), Säkerhetsskydds-
förordningen (1996:633) and Sekretesslagen (1980:100). In general these explain what
information that is classified and regulations about how this information should be handled.
The Swedish laws are all-embracing and rather general, but served as a foundation when more
specific documents regulating the Armed Forces activities were written.

2.4.2 Armed Forces regulations
Based on the legislation the Swedish Armed Forces has issued regulations that govern the
organization activities. These are documented in Försvarets författningssamling (FFS),
Försvarets interna bestämmelser (FIB) and Försvarmaktens allmänna råd (FAR). These
documents are set by the Supreme Commander of the Swedish Armed Forces.

The documents in particular, that affect command and control systems are:
- Försvarmaktens föreskrifter om säkerhetsskydd, FFS 2003:7
  (Armed Forces regulations about protection of security)
- Försvarmaktens föreskrifter om signalskyddstjänsten inom totalförsvaret FFS 2005:2
  (Armed Forces regulations about communication security)
- Försvarmaktens interna bestämmelser om IT-verksamhet FIB 2006:1
  (Armed Forces internal directions about IT related activities)
- Försvarmaktens interna bestämmelser om IT-säkerhet FIB 2006:2
  (Armed Forces internal directions about IT-security)

These documents specify among other things the levels of security classification, which now
are adapted to the NATO standard for interoperability reasons. The levels are: TOP-SECRET,
SECRET, CONFIDENTIAL and RESTRICTED. Depending on which security class
information belongs to, there are also regulations how this information should be safeguarded
and what is required to be authorized to access it. The basic rules to access classified
information is that a person:

1. is assessed to be reliable in security aspects
2. has the required knowledge in security handling
3. needs the information in the preformed work

The first rule often includes a background check preformed by the authorities.

2.4.3 Swedish Armed Forces information security policy
The Swedish Armed Forces bases the information security work on the international standard
SS-ISO/IEC 17799:2001. This standard, just like DoD TCSEC, states that there must be a
policy.

This is the declaration of will, taken from the information security policy of Swedish Armed
Forces.

The overall objective of the information security of the Armed Forces is to
ensure sufficient protection of the information assets of the authority both
within and outside the country, making sure that the information required
is available to the right person in time, and in a way that is traceable.
(SAF ISP 2005)\textsuperscript{8}

\textsuperscript{8} Swedish Armed Forces Information Security Policy
It later stresses four points that correlate with the *Confidentiality, Integrity, Availability* and *Traceability* categories.

*Information security in the Armed Forces refers to securing that:*

- the information is available when necessary;
- the integrity of the information is and remains accurate;
- the confidentiality of the information is maintained, and;
- the handling of the information is traceable.

(SAF ISP. 2005)

A complete version of the information security policy of Swedish Armed Forces in Swedish is included in appendix 1 and an official translation to English is included in appendix 2.

### 2.4.4 H SÄK IT 2006

The Swedish Armed Forces has also published a handbook about IT-security named H SÄK IT 2006. This is not a governing document but it presents the information from the other governing documents in an understandable way, with examples to further increase the readability. It helps to create understanding and could be used as guidance for people working with Swedish military computer systems. It also has a good summary of which security function that affects which security aspects.

<table>
<thead>
<tr>
<th>Security function</th>
<th>Access control</th>
<th>Security logging</th>
<th>Tempest protection</th>
<th>Protection against unauthorized monitoring</th>
<th>Intrusion protection</th>
<th>Intrusion detection</th>
<th>Protection against malicious code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security aspect</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Integrity</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Availability</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Traceability</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

**Table 2. Security functions effect on security aspects.**

In Table 2, the aspects that security functions affect are marked with an x.

*Access control* and *security logging* have been explained earlier. *Tempest protection*, is the protection against emissions of signals that could be used to monitor a system from a distance. For instance the electrical signals sent out by a cathode ray tube display, which could be picked up hundreds of meters away from the source. These signals could be used to regenerate the presented picture. *Protection against unauthorized monitoring* means to prevent persons to seeing or hearing things that they are not intended to. *Intrusion Protection* is for instance the use of firewalls to prevent persons outside of the system to be able to access it. *Intrusion detection* is used to be able to detect if any unauthorized activities is performed within the system. *Protection against malicious code* is typically the use of antivirus software.

This is then used to show which mechanisms that need to be implemented to allow the system to handle classified information from belonging to different security levels.
As can be seen in Figure 10, all systems, even non classified systems should have, access control, security logging, intrusion protections and protection against malicious code. And all systems handling information classified in CONFIDENTIAL or higher must have all security functions covered. The Swedish Armed Forces demands on the security mechanisms are covered in Försvarsmakten [6].

2.5 Related Work

The area of flexible access control for armed forces is not a new area of research. A number of propositions have been made on how to solve this.

Lee Badger wrote in 1990 about flexible security override for trusted systems. It uses the Bell La Padula model and introduces the flexibility by in advance setting up a number of different security lattices. It is then possible in case of an emergency to change the current policy to a less restrictive one. This system enables a graceful degradation of the system, but has to be planned before hand. (Badger 1990)

In 1999 Dean Povey wrote a paper presenting something called optimistic security. According to him the goal of optimistic security could best be summarized by a quote from Bob Blakeley. (Povey 1999)

Make users ask for forgiveness, not permission. (Blakeley 1996)

The optimistic security model was based on the Clark-Wilson model and had the ability to undo illegitimate actions, punish the perpetrator and remove privileges. This should ensure that the system could be restored to a valid state and act as a deterrent. The author, though, does point out that such a system is best used in an environment where the cost of recovery is low compared to the cost of not granting access. (Povey 1999)

In more recent time Erik Rissanen et al. presented a system which extends the normal behavior of an access control system. In normal access control systems, an operation is either permitted or forbidden. In their system there is also the possibility of can. If an operation is labeled can, the operation could be performed by overriding the security system. This will trigger warning systems and notify an authority. (Rissanen et al. [1] 2004) They have also presented, in a latter paper, a way of finding the corresponding authority. (Rissanen et al. [2] 2004)
The problem has also been addressed in healthcare, where Ferreira \textit{et al.} in 2006 presented a paper describing a policy which allows for what they call “break the glass”. It works like normal access control policy, but with the possibility of “breaking the glass” and override the access control rules, but the actions will be monitored and reports of the committed actions would be sent to a superior. The user will be warned when trying to access out of bound information, but will get a choice to override it. (Ferreira \textit{et al.} 2006)

A more advanced method is proposed by David Keppler \textit{et al.} They have mechanisms that intervene to mediate if access to an object is denied using the ordinary access control system. Then the circumstances of the denial are checked and a number of different actions are considered;

- Data redirection – The requested data is sent to a superior who has clearance to access it.
- Request redirection – The request for access is redirected to someone with power and knowledge to do better evaluation of request.
- Data and Request redirection – The data and the request is redirected to a trusted intermediary who could evaluate the information and context and then decide.
- Elevating the subject to a clearance level where the subject is permitted to access the requested information
- Give access to a sanitized version of the requested information
- Deny access

They point out that a system like this could overload the system by transferring large quantities of data and be used as a denial of service attack by overwhelming trusted intermediaries. (Keppler \textit{et al} 2006)
3 Command and control systems

This section presents one existing command and control system, one that is on the verge to be delivered and the outline of a future command and control system. This is to show what approach that is used today and what will be used in future command and control systems. The information in this section is mainly compiled by using written documentation and written communication between the actors designing and constructing these systems. None of these systems were available for hands on testing. The reason for this is that they are in a gap between two systems right now.

3.1 Factors

The development of command and control systems was only until a couple years ago often system dependent. This means that different fractions of the armed forces was using specialized command and control systems delivered together with their system platforms. This did not always enable cross platform communication. This is of course ineffective and together with the development of network computing in other parts of society, demands rose that different system should enable cooperation between units. In addition to this more and more military operations are performed by multi nation coalitions, which increases demands on cooperation or what is known as interoperability.

Interoperability – The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. (US DOD 2001)

Another thing that has changed is that previously, the defense industry was pushing the limits of technology, sponsored to a great extent by military and governmental funds. Now a days commercial factors drive development of technology in such a pace that the military cannot keep up with. This has created a market where the military in some cases use commercial products: called COTS (Commercial Off The Self).

3.2 IS MARK

The current command and control system used by the Swedish Army is a collection of systems called IS MARK (Informationssystem MARK). This system was originally intended to be a platform to enable experiments and testing of technology and methodology used in command and control systems. It is a part of HP ATLE, which is an acronym for the main project for army tactical command. (swe. Huvudprojekt Arméns Taktiska Ledning). (Försvarsmakten [7])

The system is based on COTS, ordinary computers as clients and servers, running Windows NT. The computers are connected by a tactical internet, which basically is a mobile network infrastructure with the capability to transport TCP/IP packets. (Ibid)

Each system has a core which provides applications to handle message transportation and functionality to synchronize the common situation picture. Messages and the common situation picture are distributed to users by replication of data in SQL databases. (Ibid)

10 IS MARK Systembeskrivning
3.2.1 Access control in IS MARK

In the security description of IS MARK, it is pointed out that functionality was prioritized over security in the beginning, and that IS MARK is not intended to be used in live operations. Further more: IS MARK is only approved for non-secret information. (Försvarsmakten [8])

In IS Mark the standard access control of Windows NT is used. Almost all system users have the same permission except system administrators and a few others. Standard Windows authentication is used with a personal login, to enable tractability of committed actions in the system. (Ibid)

3.2.2 Role handling in IS MARK

In IS MARK there are support for roles, these roles are not used as part of the security solution, i.e. the system does not use RBAC. They are mainly used to support the message handling process, and on some occasions to decide which tasks you are allowed to perform. (Försvarsmakten [9])

The reason a role based approach for message handling has been chosen, is to ensure that messages end up at the person occupying the concerned position at that moment in time. The role structure is the same at all command posts and is based on activity processes of a staff. (Ibid)

After logging on to the system and starting the IS MARK application, the users can choose which roles that they are occupying at the moment. One person can occupy multiple roles at any given time, but a role can only be occupied by one person. To ensure that roles are released upon system failure or disconnection, there is a monitoring process which releases roles when a problem is discovered. (Försvarsmakten [9]) (Försvarsmakten [10])

The roles are ordered in a hierarchal way to reflect the organization. This enables superiors to handle and read subordinates’ messages. If a message is sent to a role, which is unoccupied, the message is redirected to the nearest superior. There is also one role which enables you to monitor all message traffic to and from your unit, but this role does not allow seeing the content of the message. This role will also receive all the messages to which no recipient could be found.

Within the program you have the possibility to choose your main role, if you occupy multiple roles. This role will be used as sender for messages.

3.3 Swedish Command and Control Information System (SweCCIS)

The Swedish Armed Forces are currently developing a new version of their command and control system. It is called SWECCEIS (Swedish Command and Control Information System). The system contains two parts, one common platform that is called StabIL which provides the basic command and control services. This is complemented with Functional Area Services (FAS) which provides specialized support depending on the area of use, for instance legacy systems or platform dependent systems. The structure of the different parts can be seen in Figure 11. (Försvarsmakten [11])

---

11 IS MARK Säkerhetsbeskrivning
12 IS Mark Användarmanual
13 IS MARK Drifthandbok
14 SWECCEIS PTTEM (preliminary tactical technical economical objective)
SWECCIS aims to provide support in tactical and operational command and it has been designed to support international operations. It is presumed to be used in an environment where a command post is based either on one or on several distributed locations. Each location has the ability to work autonomously.

The goal is to have the system fully operational in 2009. When the system is operational it is supposed to be the command and control system that is fully operational at all times and used in real missions. (Försvarsmakten [11])

The first part of the system is delivered to the Swedish Armed Forces this year.

### 3.3.1 Main functionality

SWECCIS main functions are to support planning, task oriented command and control and information supply. This is mainly done using the common operational picture and the message handling system. In addition to this SWECCIS also provides tools for ordinary office work, such as a word processor, spreadsheets and presentation software. (Försvarsmakten [12])

SWECCIS uses what they call *actors*, which is defined as a person, organization or machine that affects the situation. In most cases an actor is a military unit. All information on an actor is stored in what is called an *actors card*. This could for instance include type of actor, activity, location, supply levels and preparedness levels. (Ibid)

The common operational picture is built by replicated data from different units. It is supposed to give common situation awareness. The information is presented to the operator with geo-information (maps of different kinds) as a background and the chosen objects from the database. All changes should immediately affect all operational pictures within the command post. Other command posts may have a different operational picture because each command post has rights to decide what their operational picture should look like. This is done by

---

15 Kravspecifikation SWECISS 2008
assessing information exchanged between command posts and only accepted updates are added to the operational picture. (Ibid)

The message handling system should have similar functions as email and the messages are addressed to an actor and a command-role. The messages could include attachments that could comprise of any type of object handled by SWECCIS, for instance maps, files, observation reports and actors card. The attachments could either be accepted or rejected. If accepted they will automatically be included in the command posts database and affect the operational picture. (Ibid)

3.3.2 Roles
In SWECCIS all users are called SWECCIS-operators and each operator has a job function (commission) within an actor. The operator with a certain commission then has the permission to acquire one of the available command-roles. The command-roles are ordered in a hierarchical structure to reflect the organization. Settings could be connected to each command-role, for instance which information that should be presented in the operational picture. (Försvarsmakten [12])

One command-role could not be acquired by more than one operator at a time. One operator cannot acquire more than one command-role at the same time, though it is possible for one command-role to handle other command-roles messages. There is also a function to delegate the handling of a roles message to any other command-role. (Ibid)

It is stated that by using the same role structure in all actors using SWECCIS, it will diminish the amount of system administration and be easier for users; because they only need to learn one structure of roles. (Försvarsmakten [12])

3.3.3 Security Requirement
There are some objectives concerning security specified in the preliminary tactical technical economical objective for SWECCIS these are listed here.

- The system should be able to handle information up to the classification level SECRET.
- It should be possible to define commissions and which command-roles these are able to acquire.
- There should be a log of which operator had which role at a certain time.
- System administrators should be able to see who is logged on to the system and which role they use.
- It is stated that the possibility to connect the access control system to the command-roles should exist.
- The operators should be able to change roles without logging out of the system.

(Försvarsmakten [12])

3.4 Future system (FMLS 2010)
There is no need to say that technology evolves in a horrendous speed, and that is why the Swedish Armed Forces in parallel to SWECCIS looks a bit further. This is done in a project called FM Ledsys. And their current big project for command and control systems is FMLS 2010, Armed Forces command and control system 2010 (Swe. FörsvarsMaktens LedningsSystem 2010). The objective of FMLS 2010 is to develop systems and concepts that
can be incorporated into an operational system by the year 2010. The work is mainly carried out through four different projects.

**Ledsyst T**, Technology, includes the technical parts of the future command and control system. The technical systems should be modeled as small systems with a common architecture to enable information exchange. The Swedish Defense Material Agency (swe. Försvarets Materielverk, FMV) is in charge of this program which also includes defense material suppliers. (Försvarsmakten [13])

**Ledsyst M**, Methodology, includes the evaluation of command and control staff methodology in network centric warfare on all levels, from the private soldier to the operational level. The work should be done in cooperation with the other project and its goal is to elucidate the demands on the other projects. The result should be presented as doctrinal changes, method handbooks and instructions. (Försvarsmakten [13])

**Ledsyst P**, Personnel, is to handle the changing need of human resources and competences demanded by the introduction of network centric warfare. They are to specify the needed competences and present relevant education for all personnel. (Försvarsmakten [13])

**Ledsyst O**, Organization, shall evolve the organizational models to be suitable for the command organization. They have only just started their work since they needed input from the other projects. (Försvarsmakten [13])

Much of this work is done in a new command and control development center in Enköping, Sweden. This is done in cooperation between the Swedish Armed Forces, Swedish Defense Material Agency, Swedish Defense Research Agency (swe. Totalförsvarets Forskningsinstitut, FOI) and suppliers of defense material. They work together in *Integrated Project Teams* (IPT) to present solutions to a specific task. The work is done in an iterative evolutionary way, where solutions that prove themselves useful and robust are transferred into operational systems and others are refined further or discarded.

The goals for the *Ledsyst* project are:

1. Evolve the ability to observe, orient, decide and act (the OODA-loop)
2. Create possibilities to in a flexible way be able to join, deploy and adjust deployment forces to be able to deliver the necessary abilities in operations.
3. Evolve the ability to gain efficiency in operations by increased precision and synergy effects between different functions.
4. Create prerequisite for a quick, cost efficient and evolutionary development process for all function’s development within the Armed Forces.
5. Create the requisite security in handling of resources of the Armed Forces.

(Freely translated)

1. Utveckla förmågan att sammantaget upptäcka, bedöma, fatta beslut och agera
2. Skapa möjligheter att flexibelt kunna sammansätta, insätta och anpassa insatsstyrkor för att kunna leverera nödvändig förmåga för insatser
3. Utveckla förmågan till ökad effekt i insatserna genom förbättrad precision och synergieffekter mellan olika funktioner

---

16 Preliminär målsättning för försvarsmaktens ledningssystem 2010.
4. Skapa förutsättningar för en snabb, kostnadseffektiv och evolutionär utvecklingsprocess för all funktionsutveckling inom Försvarsmakten

5. Skapa erforderlig säkerhet vid hantering av Försvarsmaktens resurser.

(Försvarsmakten [1])

The first goal is intended to increase the possibility to gain decision superiority, there is also an intention how this should be done.

*The development of command and information-management should be founded in a command-philosophy that is characterized by power of initiative, independent decision making, individual responsibility and mutual trust between all personnel within as well as outside of the organization. It should result in an increased will to accept responsibility and minimize the circumstances that impede or limits individual actions. (Freely translated)*

Utveckling av ledning och informationshantering skall grundläggas i en ledningsfilosofi som präglas av initiativkraft, självständigt beslutsfattande, individuellt ansvarstagande och ömsesidigt förtroende mellan chefer och personal samt mellan befattningsshavare på olika nivåer och organisationer. Den skall leda till att viljan att ta ansvar ökar och minimera omständigheter som begränsar eller hämmar individuellt agerande. (Försvarsmakten [1])

The second goal emphasizes the importance of interoperability and modular design which enables a easy creation of mission specific forces, national as well as international.

The third goal aims at the gist of NCW, to be able to coordinate the effect of different units to combine mission specific abilities. This should give a combined effect, which is larger than the sum of the units themselves.

The fourth goal specifies that modular design methods should be used to create the ability to quickly adopt the systems to new demands and a system which could be developed without completely rebuilding the system.

The last goal states that all resources must be handled with care to avoid unnecessary consumption or loss of them. One such resource is information which will be treated in the next section.

**3.4.1 Information security in FMLS 2010**

Information security is part of the last goal specified for FMLS 2010: protecting recourses. One of those resources is information. In FMLS 2010 information security is defined to be:

*The ability to maintain the wished level of confidentiality, integrity, availability, traceability and non-repudiation, regarding time and space, during the information’s lifespan, where the information can represent speech, pictures, text as well as sound. (Freely translated)*
Förmåga att upprätthålla önskad konfidentialitet, riktighet, tillgänglighet, spårbarhet och oavvislighet, med beaktande av tid och rum, under informationens hela livslängd och oavsett om den är i form av tal, bild, text eller ljud. (Försvarsmakten [14])

The security requirements for FMLS 2010 are classified and have not been used as a source for this thesis. There is however an unclassified document describing the collection of security goals. (Försvarsmakten [13]) (Försvarsmakten [14])

- Secure information handling is an effect of well established and used systems. It should be managed by coordinated measures in all areas; method, organization, personnel and technology.
- The solution includes functions, mechanisms, organization and methods to permit a secure handling of information up to classification level SECRET.
- The security solution has its centre of gravity in protecting information objects.
- Permissions should be based as well on roles as on individuals, it should be adaptable to support directive control and mission based joint operations.
- In each situation it should be possible to trade the level of security against the need for efficiency within the system.
- Users should receive enough unprocessed data to be able to judge the quality of the information.

The things that separate this system from the other systems are that this system should be able to trade the level of security against the level of availability dynamic and have some sort of information quality measurement tag. (Försvarsmakten [14])

3.4.2 Role handling in FMLS 2010

The notion of roles should be used in FMLS 2010. It also states that one person should be able to act as one or more roles depending on the situation and current mission. The role should be the connection between the individual and the resources which he or she is allowed to use. Connected with each role there is a role description which states the permissions and responsibilities that belong to each role. (Ackzell 2005)

To be able to create this in a convenient way there should be a number of template roles that is predefined so that the normal roles of a unit exist before hand. In addition to this it should be possible to ad extra roles or modify existing ones. (Försvarsmakten [15])

All message handling is performed between roles. The reason for this is to give the current holder of a role a possibility to access messages sent to and from the role before the holder entered that role. This is important since different individuals act as the role during time. (Försvarsmakten [15])

There is also a demand that a superior should be able to delegate process and thereby roles to another person in below him in the organizational hierarchy. (Försvarsmakten [15])

---


18 Direktiv FM LEDSYST 2006 – Rollbegreppet inom FM ledsstutveckling
3.4.3 Workgroup roles and permissions

To be able to evaluate what technologies and methodology that should be implemented in FMLS 2010 a number of so called demonstration-activities have been planned and performed. The goal is to show proof of concept for new approaches and to learn how to develop and use complex system of systems. This year one of the questions at issue was how to handle roles and therefore a workgroup has been formed to address this issue.

The method for using roles and permissions should have its foundation in *Integrated Dynamic Command and Control*. \((IDC^2)\). IDC\(^2\) is the collective result of Ledsyst M. The work is continuously updated and its purpose is to create a workflow for acting in command. It is based on two main ideas: increased comprehension and increased flexibility. (Försvarsmakten [16])\(^{19}\)

In appliance with IDC\(^2\) the method for handling permissions and roles are suggested to be handled in the cognitive domain. This means that there should be little technical hindrance and that the individual through training and education should know the boundaries and do not exceed them unless necessary. (Ibid)

In their work they distinguish between the role and the job function (commission) an individual has. They think of a commission to be closely coupled to the organization hierarchy where the role is more closely connected to the performed task. This is why they recommend that permissions are connected to roles instead of positions. They also think of roles to be the natural connection between resources and actors. Resources can for example be personnel, fire support, transportation capabilities or bandwidth. As always resources are limited, and there must be a way of prioritizing how they are used. In military tradition this is done using the hierarchal system. But the workgroup think that a connection to roles and mission will increase the ability to adapt to the specific need.

The workgroup also performed an experiment at “DEMO 2006 autumn” among the questions to be answered were these:

- Can the resource allocation be done through self-synchronization or does it need a central decision?
- How can a resource negotiation dialog be done?
- How to distribute mandate to take decisions in respect to roles and resources?
- How can roles and permissions be delegated and by whom?
- How is decision taken, regarding access to a certain service or information?
- How to handle temporary composite command teams?
- Is the individual competence safeguarded in an effective way, when using roles?
- Which principle should be used to regulate permissions
  a.) Define what is allowed and what is possible\(^{20}\) to access, everything else is denied
  b.) Define what is allowed and what is denied, everything else is *possible*.
  c.) Define what is denied and *possible* and let everything else be allowed.

Unfortunately, the results of the experiment were not available when this thesis was published.

---

\(^{19}\) IDC\(^2\) ver. 624

\(^{20}\) *Possible* here means that the action is normally denied but could be overridden by an application with a motivation.
4 Model system

As part of the result of this thesis a model for handling roles within a command control system and more specific how to handle vacant roles is presented. The model is a compilation of the model objectives (Appendix 3) and the results from research that were found when writing this thesis. It has intentionally been made on a non technical level to be comparable with the other systems examined.

4.1 Overview (Executive summary)

The model suggests a more fine-tuned classification of information than current systems. It uses the same security clearance levels as before, but recommends a further partition within each security clearance level, using lattices, to be able to provide security based on a need to know basis, for instance mission security\(^21\).

To achieve traceability all users must authenticate themselves as an individual at system log on. Individuals are assigned to one or more roles which in turn will be connected to permissions. By this the assigned roles decide what information and services that will be available to each user.

In the model there is an organizational chart, the command structure, built up by command-roles which reflects the responsibility and line of authority. The command-roles are in turn related to one or more roles. Command-roles are the foundation for message handling and the execution of orders within the command and control system.

The command-roles can be delegated according to a certain schema and in case of absent superiors certain users can extend their rights temporary. This is done on command-role basis, i.e. the user gets permission to enter another command-role to be able to solve the current mission.

4.1.1 Model definition and relations

To understand the model, a few things need to be clarified. As before the role is a semantic construction around which an access policy is formulated. Permissions are authorized for roles and roles are authenticated for subjects in many to many relations, see Figure 12.

![Figure 12. Normal role relations](image-url)

To be able to meet specific demands on a command and control system, a more complicated model is needed; the model is shown in Figure 13.

\(^{21}\) Only those taking part of the specific mission, has access to information concerning it.
In the model the roles are process oriented i.e. the permissions needed to perform one task gathered into one role. Multiple roles could then be combined to create a suitable collection of permissions for one subject. Where possible the roles can be arranged in such a way that inheritance of roles could be used to minimize the number of roles needed.

The model also has a structure called command-structure, consisting of command-roles, which describes the structure of command: the hierarchy model of responsibility and the line of authority within the organization. The structure serves several purposes. The command-structure is a natural foundation for resource management, message handling and issuing of orders in the command and control systems. It is also used to handle delegation and vacant roles.

A subject is allotted one or more roles depending on its function. Additionally the subject might also be able to acquire one or more command-roles. Each command-role automatically allots the user additional roles. Each command-role can only be occupied by one user at the same time. However there is a special type of command-role called shadow role. A user upholding a shadow role has the same permissions as the command-role it is connected to, but is not part of the command structure. This is used for instance to support a commander with a task without introducing any doubt on who is in charge.

### 4.2 Command-structure

The command-structure is created to reflect the lines of authority within the organization. It consists of command-roles which are modeled out of the different job positions (commission) that exists within a command and control system.

#### 4.2.1 Command-role

Each command-role is related to a number of roles which in turn is related to individual permissions. The command-role could be seen as a set of roles to fit a certain job function. This will simplify the proper allotment of permissions and be the foundation for delegation and overriding the access control.
Users acquire command-roles after login on to the system. The command-roles could later be dropped or added roles to suit their current tasks. There is a function that prevents users from acquiring occupied command-roles or command-roles which they do not have permission for.

One user can acquire several roles at the same time, but one command-role could only be acquired by one user at the time. This is to be able to conclude who is in charge and responsible for actions committed.

### 4.2.2 Shadow-roles

If two or more users need to have the same permissions at the same time, for instance to cooperate on a task, they could do this using *shadow-roles*. Shadow-roles are a model specific concept. Shadow-roles are a copy of the commander’s original role. The shadow-role allots, and the user associated to it, the same roles, though the same permissions, as the original command-role. Shadow-roles allow multiple users to have the same permissions in the system without risk of confusion about who is in charge. To place the shadow role within Barkas and Shandhus model of role-based delegation, it would be classified as a temporary, single step, non-monotonic delegation, see Figure 7 and section 2.3.4.

### 4.2.3 Presence system

The occupied roles will be presented in a way similar to instant messaging systems (like ICQ or MSN messenger). This is called presence presentation. The presence presentation could also be used to monitor that important roles are manned by someone. Should such a role be unoccupied for a certain time, a notifying message could be sent to all individuals with permission to acquire the concerned role, or a central authority.

### 4.2.4 Message handling

The command-role is used for addressing messages between users. Messages could be exchanged by e-mail, instant messaging or database replication, the model does not specify this. But only the command-roles are the possible recipients.

### 4.2.5 Common operational picture

The information presented in the common operational picture is also based on which command-roles that the user has acquired. These settings could then be adapted to suit personal needs and will be saved for each combination of user and command-role.

### 4.3 Role Based Access Control

The model has chosen to work with role based access control and the main reason for this is the simplified managing of permissions. There is more often a change of user on a position, than changes in the positions permissions. So if the permission is set up once, based on roles, the only thing that needs to be administered when changing shifts is the relation between the person and the roles.

The model permits a user to occupy multiple roles at any time. This does not imply that one user performs several peoples’ duties, the roles are created based on the task the role is supposed to perform, not the position (commission) within the organization.

#### 4.3.1 Inheritance

The model splits the command-structure from the role-structure. One advantage of this is that inheritance of permission could be used in the role-structure. Roles in the role-structure are created from a business model of activities. Where it is possible that the roles are structured to
permit inheritance. This will reduce the number of roles needed and create a significant reduction of relations between roles and permissions. This will make administration easier and follow the principle of simplicity.

4.3.2 Constraints
On some occasions there is a need of constraints to enforce procedures stated by the policy, for instance to enforce the principle of separation of duties. Separation of duties can for instance be used when giving a person the right to acquire a role which formerly was not allowed for him to acquire. One role initiates the process, by sending a request to promote the user in mind to another role. If this role agrees to this, the process could be performed. This could be one way of obstruct wrongfully augmentation of rights.

4.3.3 Chosen RBAC framework
Since both inheritance and constraints is used it gives that RBAC-3 is required to support the requirement on the system, see section 2.3.3 for detailed information.

4.3.4 Role Acquirement
When users log on to the system they are allotted a set of roles to reflect their personal needs. Then they have the possibility to acquire one or more command-roles which will allot them additional roles to reflect their job functions (commissions) needs.

4.4 Information classification
The laws and regulations specify demands on how to handle information in the different classification levels. The different security levels are today separated physically and in some cases on a logical level by using virtual private networks. If information is to be transferred to a lower security level it needs to be sanitized to avoid a breach in confidentiality.

The model suggests following the same regulations and practices as before but further partition the information using security lattices. This has its problems and is discussed under problem areas (section 5.3), but that is out of the scope of this thesis. The reason for partitioning information is to be able to have a need to know policy where information only is available to the users that needs it. This could be used to ensure mission security where only the participating parties get information about operations. Non-secret information does not need to be partitioned and should be regarded as freely distributable.

4.5 Traceability
The users of the systems are authenticated as individuals; which is preferred from a legal point when responsibility for actions is called upon. The individual users do not have the rights to do anything, but to assume one or many roles or command-roles. The roles assumed directly or trough command-roles are then used to control what permission the user will have within the system.

When a user assumes and leaves a role or command-role the event is logged. By logging it will be possible to see which person have committed specific actions, in the character of the role.

4.6 Override
The model specifies that there should be methods to acquire non-authorized roles under specific circumstances. Which circumstances that is sufficient for overriding the system, is a
policy question which this thesis does not give any answer to. There are, however, a number of different ways of how this could be handled. Some are presented here.

4.6.1 Delegation

If a commander knows he or she will be absent for a certain time, the commander can delegate a command-role to another user. Both the duties, tasks and the permissions are delegated to the new user. This is done by choosing a command-role and a user from an interface. The system then adds permission for the user to acquire the command-role and allot the command-role to the intended user. This is handled in a similar way in the real world, where an employee gets a mandate to handle the manager’s duties during holidays. This would be called a temporary, single-step, monotonic self initiated delegation, when using Barka and Shandhu’s model, see section 2.3.4.

From a security point of view delegation affect confidentiality and integrity, by letting non-authorized user access information normally handled by the commander. The model suggests therefore that delegation only should affect information and services on RESTRICTED and CONFIDENTIAL security classification levels. The reason it should be allowed there is that if the commander trusts the appointed person the system should not be of hindrance. On higher security clearance levels the information could be too sensitive to allow for such a discretionary approach. To give the delegated member permission to access information on these levels a central authorization is needed, see further down. You might also want to have a restriction that the delegated member is part of the same branch in the command-structure tree.

When an intended person gets a command-role delegated, that person will be forced to acknowledge the delegation. In doing so, the user is made aware that new duties have been added. This will work as a re-authentication and could be used to state non-repudiation and could also counter that a role is delegated to a person which have been compromised. This is called a bi-lateral agreement in Barka and Shandhus model.

If a commander needs help with a task from someone that does not have the required permissions, but still wishes to remain in charge, he can delegate a shadow-role to the intended person. A shadow role will transfer permissions, to the user, while maintaining the commander’s authority. A definition of shadow-roles could be found in section 4.2.2.

4.6.2 Initiative

Initiative is another model specific notion. The foundation for this is that any member of a unit should be prepared to take on the responsibility as a leader of the unit if necessary. This is a temporary solution until there is time to sort things out.

If a superior is not available and there is need for some action that could only be performed by the superior, any of his subordinates could try to acquire his command-role. This is done using the usual interface for requesting command-roles. There are three different ways that an initiative could be handled.

- Trusted user
- Non-trusted user, using trusted representative.
- Central authorization
The superiors have made a list in advance of trusted subordinates. If a subordinate requests a command-role for which he or she is trusted, he or she will be allotted the command-role. This could be compared to Barka and Shandhu’s delegation-model expression, agent-delegation, but this aspect was not covered in their model. They did not allow for trusted persons whom they call agents, to delegate a role to them self, which this could be translated into, see section 2.3.4.

If the subordinate is not trusted, a request will be sent to the available trusted individuals, who will decide if the subordinate should be allotted the command-role or not. This is also similar to the agent-delegation case as described by Barka and Shandhu (2000), but the initiation is done by the user which requests a delegation to him- or herself.

If a non-trusted user requests a role for which there are no trusted persons available, the request will be forwarded to a central authority for manual handling.

When someone tries to access a role which they normally do not have permissions to, they will be presented with a message, stating that they are overriding their normal permissions and that a more extensive logging will be made. The message will require a signature, in form of an authentication, to verify that you have understood the message and are willing to accept the responsibility and take consequences for your action. This will ensure non-repudiation.

### 4.6.3 Central authorization

Central authorization is the normal way of handling users’ rights in ordinary systems. Requests to acquire unauthorized command-roles/files will be sent to a central element for evaluation by a person who then forwards the request to a proper instance which makes the actual decision. This could then be effectuated by the central authority. It is important to point out that the decision should not be taken by the central authority; it just mediates the request to the instance with knowledge and mandate to decide and then effectuates their decision. This is basically what an ordinary system administrator does.

In the model central authorization is used together with the other methods, as a way of last resort. It can be used where no trusted persons are available or when an individual tries to delegate roles to someone outside of their hierarchical tree.

### 4.6.4 Occupied role

Like previously stated it is not possible to acquire a role that is already occupied, but in some cases there may be a reason for replacing the holder of the role. This is handled in the same way as initiative, but the current role holder will be downgraded to a shadow-role. There is also a function that monitors for inactivity and loss of connection. If an individual is unavailable or inactive for a certain time, the roles connected to this person will be dropped.

### 4.6.5 Restrictions

The security clearance level is bound to the individual and is not inherited on delegation and initiative. Since the regulation demands actions that has to be done outside of the system, for instance background checks, this has to be done by central authorization.
5 Discussion
Different thoughts have emerged when looking at the present and future command and control systems. Here those thoughts will be presented and discussed. These thoughts have then been the foundation when motivating decisions in creating the model.

5.1 Vacant roles
Vacancy can be a problem within organizations. The examined systems have different approaches on how to solve this issue. These approaches are presented here.

5.1.1 IS MARK
Since IS MARK does not use roles to control the access control system, the only instance where vacant roles could be a problem is in message handling. This has been solved by redirecting messages from vacant roles to their superior and having a general postbox in the top of the hierarchy, which always is under supervision by someone. This seems to be an adequate solution to solve the message handling problem.

5.1.2 SWECCIS
SWECCIS is stated to work in the same way as IS MARK, concerning message handling. But there is one difference; a role could delegate the right to handle its messages to any other role. This could be used to handle planned vacancy in a more appropriate way than the IS MARK. This lets an appointed role handle the messages instead of a superior which could be overloaded in an organization with many vacancies.

SWECCIS also suggests roles to determine access control permissions. No information however has been discovered that supports how this connection should work. The same goes for any information about vacancy handling. In addition to this SWECCIS only permits one-to-one relationship between operators (users) and roles, this will complicate a situation where someone should take over someone else’s role since he or she need to leave the role he or she is currently upholding, which only means moving the vacancy.

5.1.3 FMLS2010
In FMLS2010 they have identified roles, as an area which must be handled. But their focus is more on adjusting roles to support the workflows and tasks. They have their foundation in the command method called IDC^2, which sees everything as a continuous work adopting the methods to the current situation. They recommend that roles are handled according to IDC^2, where roles are adopted as the mission and current situation evolves. In order to minimize the amount of administration, the main thought is to give each user as large degree of freedom as possible and then rely on the users’ discretion not to use their abilities in wrongful ways.

The experiment done during “Demo 06” handled hierarchies and role permissions. One question was if roles should be defined prior to deployment or if this should be part of the staff process, i.e. the staff finds their own roles and act accordingly. The question indicates that they have identified vacant roles as a potential problem but have not found any concrete suggestion on how to solve the problem.

5.1.4 Conclusion
When looking on the different existing and future systems it seems like vacant roles are a problem, but it could be dealt with in different ways depending on the context.
In message handling, the problem could be solved by methodology, and minor technical mechanisms. By forwarding messages to someone present, the message is managed by someone, who might not be the intended recipient, but it is better than no recipient at all. The feature included in SWECCIS; to be able to choose who will manage vacant roles messages, is an improvement compared to IS MARK.

The real problem with vacant roles arises when roles are used as foundation for access control systems. The idea of an access control system is to limit subjects’ access to objects, for some reason; otherwise the access control could be removed. If a vacant role which has exclusive permission to access some information and somebody needs that piece of information, there could be a problem. The model suggests a couple of methods to circumvent the access control but still maintain some degree of security. Anyone cannot be allowed to override the access control, because this would render the access control system pointless.

5.2 Overriding access control

In the real world persons sometimes do things they are not formally allowed to do, because the situation calls for it. The question is how to implement this into a command and control system, in an orderly way. An orderly way means that it provides the flexibility of the real world without sacrificing to much of the security. In most systems a manual approach, or what the model calls central authority, could be used to override the access control system. What is sought here is a prepared way to decide if someone should be allowed to extend their permission to speed up the process.

In IS MARK the need for an override function is superfluous, since almost all information is accessible to all system users.

SWECCIS has the demands of being able to handle classified information up to the level SECRET, so at least there is some classification of information. Since changing the security levels on information or users is a process that could take some time, for instance security background checks, there is hardly any need for automated functions to override access control for a higher security clearance level. Within one level, if further partitioned, there could possibly be use of such a function, but noting that states the existence of such a partition or override function has been found in the documentation.

In FMLS2010, Ledsyst M recommends to eliminate as much of this problem as possible by giving each role/user as much permissions as possible and then use the manual approach to fix the remaining issues. They have adopted a methodology very close to the one Povey proposed in 1999.

The model assumes a partition of information within each security level and that the system is specified to work according to the principle of least privilege. Then situations will arise where privileges need to be extended to some roles. The two ways of overriding the normal access control that the model introduces are delegation and initiative.

5.2.1 Delegation

Delegation has its foundation in the traditional way of handling large tasks and foreseen vacancies. It is a well-known concept which correlates well with directive control where the commander issues tasks and allots resources which is what delegation is all about. This ought
to be transferred as a function into the digital domain. One weakness with delegation is that it only works in predicted situations and needs to be initiated by the superior.

From a security objective delegation is a transfer of abilities by using out of band trust. The individual that gets a superior’s role delegated to him gets this because the superior knows that the individual has the abilities and knowledge needed to handle the situation. Delegation increases availability of the information but that on a cost of confidentiality and integrity. The decision is made by the commander that delegates his role, so it is sort of a discretionary system.

One question that needs to be taken into consideration is if the individual is allowed to delegate the abilities further. This is a policy question and not considered here, a suggestion would be to only allow one step delegation since the delegating person still has the responsibility for the action made when delegating a task. You can only delegate abilities and tasks, not the responsibility.

Delegation in the form of shadow roles delegates the permission of a role without the duties connected. This is a way for a user to share his burden with another user; they can both access the same information and by this help each other to do the work of the role. Shadow roles also facilitate the handover issue when working in shifts. The individual could get up to speed by being able to access the same information as the role holder. Then on a given time, the role is transferred to the new individual, which by this takes over the duties and responsibility.

One possible threat against this scheme is that a role gets delegated to a user which has been compromised. This could be hard to control. One technical way to verify that the user is who the system claims, is to issue a re-authentication. A methodology approach would be to let the delegating person do an out of band check, for instance speak to the person.

### 5.2.2 Initiative

*Irresoluteness and lack of power to act will often have more serious consequences than mistakes in the course of action.* (Freely Translated)

*Obeslutsamhet och bristande handlingskraft får oftast allvarligare följder än misstag i fråga om tillvägagångssätt.* (Försvarsmakten [2])

Delegation has to be initiated by a superior. The contrast is when a subordinate takes command by his or her own initiative. This is a more powerful method that could be used in all situations but it also has more risks connected to it. If anybody was able to take on anyone’s role the access control system would be useless. So the gist is to allow the correct initiatives and prevent the wrongful. This is in essence the adjustment between availability and on the other side confidentiality and integrity.

The list of trusted persons is a half adoption of the delegation case, where the decision is prepared in advance to enable quick deployment later.

In the case where a non trusted person tries to acquire a role, a request is sent to the available trusted persons for this role. If any of them accepts that person, the person will be able to acquire the role. Because of the human interaction, this procedure takes a little more time than if a trusted person tries to take on the role by his or her own initiative.
If a trusted person’s account is compromised the offender could increment his rights to all the command-roles the user is trusted for. It could be partially countered by not showing what command-roles an individual is trusted for. By doing so, an offender must try to take on command-roles to see which ones that could be acquired. Requests of a non-trusted role will initiate requests, which will hopefully create attention.

If an offender uses a compromised user-account and tries to acquire a command-role which the user is not trusted for, there is a risk that requests are accepted by the trusted individuals. This could be countered by out of band verification that the person is who he or she claims to be. Request for command-roles could also be used as a denial of service attack, by overwhelming trusted persons with requests for roles. This seems to be rather futile, since this will only reveal the occurrence of a compromised user account which would be shut down.

5.2.3 Conclusions

The existing systems do not provide any specific automated functions for overriding of access control. They rely solely on the centralized handling of changes to the access control. Why do not any of these systems have such a function? It could be because they have an access control system which permits quite a lot from the beginning. Does this make the model excessive in current system? The answer to this is probably yes, but if there would be a stricter classification of information, the model could be of use. If in addition to this the principle of least privilege is used, there will emerge situations where an automatic override of the access control system is desirable.

5.3 Trouble areas

The first thing that needs to be solved is how information should be classified into different partitions. How would these different partitions be created; unit wise or mission wise? How could someone know if useful information exists in another partition? Could the division of information into partitions be done by machines? Could a human process and partition enough information in the required tempo? Does all of the above follow the principle of simplicity? No, but there are areas where you could accept a certain delay and where there are logical partitions that could be used to partition information. So the model is not useless; it only needs to be applied when these prerequisites prevails.

Another problem area is the flow of information. Basic theories behind access control systems are simple, and they could prove that information in one partition cannot leak to any other partition, if the theories are followed. This is in theory, in the real world information flows in an almost uncontrollable way. All imaginable ways could be used to transport information, there are hidden channels and there are out of band channels that could be used. An example of this is if a person reads something in one partition and then manually writes that piece of information in another partition. This violates the theory rules but without effective feedback to the user. This shows that prevention is not enough; the system also needs to be able to detect when information is where it is not supposed to be. The knowledge of which information have been disclosed could be used to take preventive actions to minimize the effect of the disclosure. Another problem with security lattices is that information can become unavailable to legitimate users. This could happen if one user creates a document within one category, say for instance category A. If this information is then updated by another user, member of both category A and B, the document will then belong to compartment AB. The document will no longer be accessible to the original creator of the document. This is meant to prevent illegal flow from compartment B to compartment A, but introduces these new problems.
To provide a good enough availability in existing systems the trivial solution has been used, to let everybody have access to all information. Confidentiality is upheld by the use of security clearance levels and in limiting physical access to the system. This is not a good design for a system which is used in the battlefield. Secrecy and misinformation has always been a cornerstone of warfare, and the information age has certainly not changed that. A system where every node is a potential way to access all resources is very vulnerable. Just like Sun Tzu said.

The spot where we intend to fight must not be made known: for then the enemy will have to prepare against a possible attack at several different points; and his forces being thus distributed in many directions, the numbers we shall have to face at any given point will be proportionately few. (Sun Tzu)
6 Results

In a system there can never be both absolute confidentiality and absolute availability at the same time, which is shown in section 2.2.1. The way this has been treated in current command and control systems is by allowing all users to have access to almost everything. A system like this is vulnerable for attacks and internal mistakes. One single mistake or exploited vulnerability could result in a complete disclosure of the systems information. To limit the effect of such an event the amount of information contained within systems could be limited in size. Unfortunately creating several small systems will cause availability issues between the different systems.

The main advantage of the model is its flexibility. The model provides a method to have information partitioned on a need to know basis but avoid the dependencies between certain individuals. The level of flexibility could be adjusted by a policy, for instance the number of possible trusted individuals or the methodology to verify that request to extend users rights is valid.

The model will also simplify the handover procedure when working in shifts, by the use of shadow-roles. Because of the model’s separation between roles and command-roles, it could still provide functionality according to command-lines, chain of authority and maintain the advantage of simplicity of administrating a role based access control systems.

The disadvantages of the model are that it is more complex than the existing solutions and the problem areas mentioned. The suggestion until better methods are discovered is to classify and tag information, in a best effort manner. Some types of information could be automatically tagged on creation, for instance unit identifier, and then use this as foundation for a category. Also the users should be able to add metadata on their data to be able to create their own category for mission security. It should also be possible to update a document and save it in a chosen category. This will open up for information flows between categories, but it will still be more secure than an all access system and prevent availability problems that occur in a strict security lattice system. If this is done, the model could be used to ensure availability within each security classification level. This gives a higher degree of confidentiality and integrity, especially at the start of a mission and still provides a lower bound for security. The lower bound is the security classification levels, which cannot be overridden by the model.

6.1 Validation

The validation aims to answer the question if the model adds any value to the existing systems. As a guideline in this evaluation the system objectives have been used, these can be found in appendix 3.

The existing systems, IS MARK and SWECIS do not have any role based access control; they use mandatory access control supplied by the operating systems. This seems to be sufficient for today’s system, because there is no reason to introduce role based access control unless there is information that should be accessible to some individuals and denied to others. In this area the model is superfluous but maybe such a partition of information will be required in future systems.

If the role-based part of the model is not used, the model still has its advantages over the existing systems.
• The command structure could still be used to delegate handling of tasks and messages.
• The presence presentation could notify persons on vacant roles and messages could be sent directly to manned command-roles.
• The use of shadow-roles would enable easier handover procedures when working shifts.

The command-structure part of the model is also pretty similar to the role structure used in SWECCIS so maybe these parts can be incorporated into future systems.

It is hard to compare the model and FMLS2010 since there is limited information about it and fundamental design decisions are not taken yet. The important thing is that they have identified both the problem with roles, delegation of permissions, and partitioning of information.

6.2 Future research

The model this thesis describes could of course be further refined and extended. One thing that could be done is to see what issues that might be incorporated into the model apart from the ones that should be handled by policy decisions. Example of such things are the ability to delegate a delegated command-role further and delegation and initiative outside of the own organizational branch.

There are also a number of different things that this thesis has touched but not thoroughly treated, examples of this is multi level security systems, detecting illegal flow of information, use of instant messaging in command and control system and automatic tagging and sorting of information into different categories. Some of these areas could be well worth exploring; the area of multi layer security has already been thoroughly explored by numerous researchers, with lots of gained knowledge, but without definite solutions. On the other hand, the usage of instance messaging in command and control system seems to be rather unexplored.

One thing that most certainly would take this work further is a closer cooperation with persons involved in developing command and control systems and people using them on a daily basis. This would give more perspectives on the use of the system and the problems of building them. A model is just a simplified theoretical product that hopefully describes the real thing in a sufficient way. Now the model is created and it is time to see if it stands up to the test.
Appendix 1. Försvarsmaktens informationssäkerhetspolicy

Det övergripande målet med Försvarsmaktens informationssäkerhet är att säkerställa ett tillräckligt skydd för myndighetens informationstillgängar såväl inom som utom landet, så att rätt information är tillgänglig för rätt person i rätt tid på ett spårbart sätt.

Information är en av Försvarsmaktens viktigaste tillgängar och utgör en förutsättning för att kunna bedriva verksamheten. Våra informationstillgängar måste därför behandlas och skyddas på ett tillfredsställande sätt mot de risker som förekommer. Lagar och förordningar utgör grunden för Försvarsmakten i detta arbete, dessutom ska ingångna överenskommelser och avtal följas.

Med informationstillgängar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.

Informationssäkerheten omfattar Försvarsmaktens informationstillgängar utan undantag.

Med informationssäkerhet avses i Försvarsmakten
• att informationen finns tillgänglig när den behövs,
• att informationen är och förblir riktig,
• att informationen endast är tillgänglig för dem som är behöriga att ta del av och använda den, samt
• att hanteringen av informationen är spårbar.

Försvarsmakten definition på informationssäkerhet innebär alltså ett vidare begrepp än det som anges i säkerhetsskyddslagen.


Var och en i Försvarsmakten ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för våra informationstillgängar.

Informationssäkerhetspolicyn förverkligas genom att vi uppnår våra mål, följer våra handlingsplaner och genomför de åtgärder som beskrivs i Försvarsmaktens regelverk.

Varje organisationsenhet är bunden av denna policy, vilket medför att det inte finns något utrymme att besluta om lokala policies som avviker från denna informationssäkerhetspolicy.

Den som använder Försvarsmakten informationstillgängar på ett sätt som strider mot denna informationssäkerhetspolicy kan bli föremål för åtgärder från myndighetens sida.

Militära underrättelse- och säkerhetsstjänsten i Högkvarteret ansvarar för att informationssäkerhetspolicyn årligen granskas och vid behov revideras.

Denna informationssäkerhetspolicy är fastställd av överbefälhavaren den 5 april 2005 och ska börja tillämpas den 1 maj 2005.
Appendix 2. The Information Security Policy of the Armed Forces

The overall objective of the information security of the Armed Forces is to ensure sufficient protection of the information assets of the authority both within and outside the country, making sure that the information required is available to the right person in time, and in a way that is traceable.

Information constitutes one of the most important assets of the Armed Forces and is a necessity for performing its duties. Our information assets must therefore be handled properly and given satisfactory protection against existing risks. For the Armed Forces, laws and ordinances constitute the basis in these efforts; in addition agreements and treaties shall be complied with.

Information assets include all information whether if handled manually or automatically and regardless of format or environment in which it occurs.

Information security in the Armed Forces refers to securing that:

- the information is available when necessary;
- the integrity of the information is and remains accurate;
- the confidentiality of the information is maintained, and;
- the handling of the information is traceable.

Hence, the definition of information security used by the Armed Forces has a wider scope than stated in the provisions of the Protective Security Ordinance.

Information security is an integrated part of the Armed Forces activities. Each who to some extent handles information assets is responsible for maintaining information security. Managers at all levels within the Armed Forces also have the responsibility to actively endeavour that all employees realise the importance of information security. Moreover managers shall promote a generally positive attitude towards security work in all activities. Information security issues within the Armed Forces are managed and co-ordinated by the Military Intelligence and Security Directorate at the Headquarters.

It is incumbent on each member of the Armed Forces to be vigilant and report incidents that might affect the security of our information assets.

The implementation of the Information Security Policy depends upon the achievement of our goals, following our plans of action and enforcing the measures described in the Armed Forces framework of regulations.

Every unit is bound by this policy, hence no local policies can be decided of that are not in compliance with this Information Security Policy.

A person who uses the information assets of the Armed Forces in a way which is contrary to this Information Security Policy may be subject to measures from the authority.

It is the responsibility of the Military Intelligence and Security Directorate at the Headquarters to annually review and if needed revise the Information Security Policy.

This Information Security Policy was approved by the Supreme Commander on 5 April 2005 and shall enter into force as of 1 May 2005.
Appendix 3. System Objectives

Introduction
In a command and control system, rights to use services or access information are connected to different roles. A person is then appointed to one or many roles. The person will then be able to make use of the permissions connected to those roles to access information and services.

Purpose
We want to specify a system which will be able to manage the role appointment process in a flexible but still secure way. It should be able to be used beforehand to configure a baseline setup. It should also be possible to later change the casting. The system should also be able to facilitate the hand-over procedure when working in shifts. The new approach of this system is that a person under some conditions will be able to extend the own or someone else’s roles to be able to solve an ongoing task.

Project scope
The system will be used in a single command and control system. The objective is to be able to connect roles with persons. And under some premises let a person take on a new role.

Overall description
The system will be an add-on on top of the operating systems mandatory access control system.

Product Objectives
- Managing the connection between persons and roles.
- Managing the connection between roles and permissions
- Logging to trace which person acted in which role during what time.
- Handling requests to acquire a role which the user is not authorized for.
- Handling delegation of roles.
- Database keeping track of the current casting.
- Method to assess if a request for a role is to be accepted.
- Method to check and present presence of roles in the system, like an instant messaging system.
- Feature controlling the uniqueness and existence of roles in the system
  - Solve collisions
  - Warn if a critical role is not appointed
- Be able to handle different security clearance levels
- Support for need to know policy
- One person should be able to occupy many roles.
- Each role should only be occupied by one person at the time.
- It should follow Swedish rules and regulations about handling of classified information.
Bibliography


**Swedish Armed Forces books and written communication**

Försvarsmakten [1], Ledsyst mål och riklinjer, HKV 09:100:77095 2005-12-01

Försvarsmakten [2], AR2 (Armé reglemente del 2) 1995.

Försvarsmakten [3], Försvarsmaktens Grundsyn Ledning. Stockholm 2001

Försvarsmakten [4], Militästrapstrategisk doktrin 2002

Försvarsmakten [5], Handbok för Försvarsmaktens säkerhetstjänst, informationsteknik. H SÄK IT 2006, 2006
Försvarsmakten [6], Beslut om krav på godkända säkerhetsfunktioner, ver 2.0, HKV 1O 750:78976 2004-12-20

Försvarsmakten [7], FUM IS MARK 06 Systembeskrivning ver 4.0 2005-09-30

Försvarsmakten [8], FUM IS MARK 06 Säkerhetsbeskrivning ver 4.0 2005-09-30

Försvarsmakten [9] Användarmanual IS Mark 1.1.3 Förbandsversion ver 8.0A 2004-09-17

Försvarsmakten [10] FUM IS MARK 06 Drifthandbok ver 4.0 2005-09-30


Försvarsmakten [14], FMLS 2010 förtydligande av målbild 2010 med inriktningar för verksamheten 2006, HKV-09 100:64336 2006-04-06


Försvarsmakten [16] Integrerad Dynamisk Ledning (IDC2) ver 624 rev 0.6 2006-09-26

**Online references**


Sun Tzu, on the art of war. Translated by Lionel Giles, M.A. (1910) http://www.gutenberg.org/files/17405/17405-h/17405-h.htm Published: 2005-12-28 | checked: 2006-06-17

52
På svenska

Detta dokument hålls tillgängligt på Internet – eller dess framtida ersättare – under en längre tid från publiceringsdatum under förutsättning att inga extra-ordinära omständigheter uppstår.

Tillgång till dokumentet innebär tillstånd för var och en att läsa, ladda ner, skriva ut enstaka kopior för enskilt bruk och att använda det oförändrat för ickekommersiell forskning och för undervisning. Överföring av upphovsrätten vid en senare tidpunkt kan inte upphäva detta tillstånd. All annan användning av dokumentet kräver upphovsmannens medgivande. För att garantera äktheten, säkerheten och tillgängligheten finns det lösningar av teknisk och administrativ art.

Upphovsmannens ideella rätt innefattar rätt att bli nämnt som upphovsman i den omfattning som god sed kräver vid användning av dokumentet på ovan beskrivna sätt samt skydd mot att dokumentet ändras eller presenteras i sådan form eller i sådant sammanhang som är kränkande för upphovsmannens litterära eller konstnärliga anseende eller egenart.

För ytterligare information om Linköping University Electronic Press se förlagets hemsida http://www.ep.liu.se/