National Defence University
Department of Military Technology
Series 3: Working Papers No. 1

SITUATIONAL AWARENESS FOR CRITICAL INFRASTRUCTURE PROTECTION

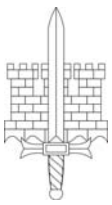
Jouko Vankka (ed.)

MAANPUOLUSTUSKORKEAKOULU
SOTATEKNIIKAN LAITOS
JULKAISUSARJA 3: TYÖPAPEREITA NO. 1

NATIONAL DEFENCE UNIVERSITY
DEPARTMENT OF MILITARY TECHNOLOGY
SERIES 3: WORKING PAPERS NO. 1

Situational Awareness for Critical Infrastructure Protection

EDITOR JOUKO VANKKA



NATIONAL DEFENCE UNIVERSITY
Department of Military Technology
HELSINKI 2015

Prof. Jouko Vankka (ed.): *Situational Awareness for Critical Infrastructure Protection*
Maanpuolustuskorkeakoulu
Sotatekniikan laitos
Julkaisusarja 3: Työpapereita n:o 1
National Defence University
Department of Military Technology
Series 3: Working papers No 1

DISCLAIMER

Working papers are preliminary works in progress that have been posted or published to stimulate discussion and comments. In addition, they provide information to the general public.

The views, opinions, findings, and conclusions expressed in these papers are strictly those of the author(s) and do not necessarily represent the views of the National Defence University. Therefore they should not be reported as such. The National Defence University assumes no responsibility or liability for the statements, opinions or conclusions expressed in these papers.

Although checked by departmental publishing boards of the National Defence University, these working papers have not been through a process of blind peer-review.

Most recent publications in pdf-format:
http://www.doria.fi/handle/10024/73990

Maanpuolustuskorkeakoulu – National Defence University
Sotatekniikan laitos – Department of Military Technology

ISBN 978-951-25-2720-5 (nid.)
ISBN 978-951-25-2721-2 (PDF)
ISSN 2343-2357 (nid.)
ISSN 2343-2365 (PDF)

Juvenes Print
Tampere 2015

Preface

Postgraduate seminar series with a title Situational Awareness for Critical Infrastructure Protection held at the Department of Military Technology of the National Defence University in 2015. This book is a collection of some of talks that were presented in the seminar. The papers address designing inter-organizational situation awareness system, principles of designing for situation awareness, situation awareness in distributed teams, vulnerability analysis in a critical system context, tactical Command, Control, Communications, Computers, & Intelligence (C4I) systems, and improving situational awareness in the circle of trust. This set of papers tries to give some insight to current issues of the situation awareness for critical infrastructure protection.

The seminar has always made a publication of the papers but this has been an internal publication of the Finnish Defence Forces and has not hindered publication of the papers in international conferences. Publication of these papers in peer reviewed conferences has indeed been always the goal of the seminar, since it teaches writing conference level papers. We still hope that an internal publication in the department series is useful to the Finnish Defence Forces by offering an easy access to these papers.

Editor

Contents

Designing Inter-Organizational SA System to Disturbances of Electricity Supply

Heidi Krohns-Välimäki
Tampere University of Technology
heidi.krohns@tut.fi

Abstract

Purpose

There have been several problems in information exchange between actors in the disturbances of electricity supply. For example in storm 2011 in Finland, a municipality had problem to contact their local distribution system operator (DSO) because they had only the phone number of DSO's customer service, which was congested. At present, the situation awareness in disturbances of electricity supply is focused on every actors own perspective. In addition, present sources of SA are shattered.

Methods

In this research, the demonstration of inter-organizational situation awareness system to disturbances of electricity supply is developed. The design process has been iterative. The usability of the first version of the demonstration has been evaluated with Nielsen's heuristic evaluation method. The needs of information exchange have been studied by user need interviews with one municipality and two fire and rescue service.

Findings

The theory of team SA is inadequate in case of disturbances of electricity supply. Different actors do not have common sub-goals. There is a need for extension of the team SA theory to cover cases where sub-goals are more likely linked to each other than common.

The designed demonstration improves information exchange between actors. In addition, it improves the resilience of society in disturbances by helping the authorities to focus their actions to sites that do not have electricity and or mobile network.

Originality

The main difference that the demonstration has to existing methods is that there is a criticality database where information about sites that are highly dependent on electricity is stored. In addition, the demonstration combines information from multiple different actors to same view.

In this research it was clarified that inter-organizational situation awareness system can change the thinking about how the restoration process of electricity distribution network in disturbances should be formed.

Keywords

Electricity supply, Disturbance, Inter-Organizational, Situation Awareness

Paper type

Research paper

1 Introduction

There have been several problems in the information exchange between organizations in disturbances of electricity supply. Usually in disturbances, municipalities and authorities receive information from distribution system operators' (DSOs') web pages, like transformer level maps or lists that show the outages and their duration and by phone conversations. The problems that municipalities and fire and rescue services have in disturbances are just a tip of the iceberg.

Widespread and long lasting disturbances in the supply of electric power has been caused by Storms like Pyry and Janika in Finland in 2001, Gudrun 2005 and Per 2006 in Sweden, four storms in the summer of 2010, storms at Christmas 2011and two storms in autumn 2013 in Finland. In those storms, some individual customers were without electricity for a few weeks in the worst cases. In addition to storms that affect the rural area the hurricane Sandy caused widespread disturbances in Eastern parts of the USA in October 2012 including some cities. There were e.g. floods that caused outage to Manhattan in New York. In January 2011 snow load on trees caused widespread disturbances in Finland. [1]-[10]

Storms and other severe weather conditions induce many of the long lasting and wide spread disturbances so called major disturbances. Nonetheless there have also been major disturbances that have not been especially long lasting but extremely wide spread, like the disturbances in the transmission systems in the USA and Canada in 2003 and in Central Europe in 2006 caused by human error. Both of these caused negative societal consequences. [1]-[10]

Typically, the disturbances caused problems in telecommunication, water supply, animals' conditions in farms and with the coldness in private houses. The coldness of the houses has led to even some evacuations. The problems with telecommunication effected also to safety phones and safety buttons. [1]-[10]

After the storms in Finland in December 2011 the Finnish Electricity Market act was changed so that DSOs should participate in the formation of a situational awareness and supply any information relevant to this purpose to the responsible authorities. [11]

In major disturbances of electricity, there are multiple actors involved, like DSOs, contractors, fire and rescue services, emergency response centres, police, municipalities, voluntary organizations and customers. All the actors are obligated to maintain their capability to carry out their duties related to major disturbance. Major disturbances cause them also more duties e.g. fire and rescue services help people out from the elevators and municipalities arrange evacuations and check if elderly people need help. [3]

In relevant studies they have noticed several problems with inter-organizational situation awareness in major disturbances in Germany. There are problems with distributed information, missing awareness about available information, policy issues of information, handling the uncertainties of information, terminology issues and perceiving interdependencies between information. The policy issues and workload issues prefer that there is no need for common awareness for every actor. Instead shared information should be individualized or localized. Same issues have been noticed also in Finland. [1]-[6], [12], [13]

In this research a demonstration of the situation awareness system has been developed to improve inter-organizational situation awareness in disturbances of electricity supply. Demonstration consists of an internet service which combines information about disturbances in the electric power supply from DSOs' information systems and information from other actors. The demonstration illustrates how the exchange of information between actors could be executed by using a situation awareness system. In addition to present ways, the demonstration has a database which contains information of customers highly dependent on electricity. Usability of the demonstration has been evaluated by using heuristic evaluation. For further development of the demonstration, municipality and two fire and rescue services were interviewed to clarify the user needs. The results of the heuristic evaluation and the interviews have been analysed and further development needs have been noticed. The design process of this demonstration is presented on this paper.

2 Disturbances of electricity supply

2.1 Structure of the electricity networks in Finland

Finnish electricity network can be divided to three different parts; transmission network, distribution network and low voltage network. The transmission network transfers electricity from power plants to different parts of Finland and it is operated by Transmission System Operator (TSO). The voltage levels in this network are high; from 110kV to 400kV. The transmission network consists on overhead lines. It is not sensitive to outages, because the poles are high and is not located on the tree lines. However, if there is an outage in the transmission network it may cause whole Finland, because all smaller electricity networks are attached to transmission network. [14]

Distribution network indicates smaller electricity networks that transfer electricity from transmission network or from smaller power plants to low voltage networks. There are approximately 80 Distribution System Operators (DSOs) in Finland and

they have own operating areas. DSOs own the low voltage networks as well. The low voltage networks transfers electricity from the distribution network to customers. Usually the low voltage networks are short and there is only few customers attached to the same line. [14]

The distribution networks are the most sensitive networks to outages. There are multiple customers attached to transformers of the distribution network. At present, the most of the distribution networks consist on overhead lines nearby the tree lines. However, nowadays the most of the DSOs are replacing the old overhead lines with cable and all the new lines are built as a cable. [14]

2.2 Disturbances of distribution network

In Finland, the most of the widespread and long lasting disturbances in electricity supply are caused by weather e.g. storms, snow loads or lightning especially outside the cities. The distribution network consists on radial lines. If there is a fault in line, relay will trick the whole feeder. Usually there are multiple customers connected it. Last year customers had approximately 4 hours interruptions in total. [15]

When the disturbance is caused by storms the weather is usually causing problems to restoration process e.g. trees or lot of snow on the streets. In Finland, there have been many long lasting disturbances in last decade. In this research, a major disturbance in the supply of electric power was defined as a long lasting or widespread interruption in the supply of electric power, during which the fire and rescue services and one or more other public actor (municipality, police, etc.) need, in addition to the distribution system operator (DSO), to start implementing measures for reducing possible severe consequences to people and property. [4]

The characteristics of the most relevant major disturbances are shown in Table I. In the 2011 storms were the expenses for the whole Finnish society were the most substantial ever.

The societal problems caused by these major disturbances have been similar. There have been problems in water supply and sewerage, interruptions in telecommunication networks, and problems in farms with animals. There have been huge problems with information exchange between the actors e.g. in one storm the local DSO did not had information that one site was retirement home they thought that it was a regular household customer. On other case, the fire and rescue service could not reach the local DSO, because they had only the public customer information phone number and it was congested. [1]-[7]

Table I. Major Disturbances as Numbers [16]-[26]

Major disturbance	Amount of interrupted customers	Longest interruption experienced by a customer	Total costs of distribution system operators	Compensations paid by insurance companies	Forest damages
2001 (Pyry, Janika)	860,000	Over 5 days	Over 10 M€	n/a	Over 7 Mm^3
2010 (Asta, Veera, Lahja, Sylvi)	480,000	42 days	32 M€	81.5 M€	8.1 Mm^3
2011 (Tapani, Hannu)	570,000	Over 14 days	71 M€	102.5 M€	3.5 Mm^3
2013 (Reima,Eino, Oskari, Seija)	400,000		44 M€	20 M€	

2.3 Actors in disturbances

In this research it has been noticed that main actors in disturbances of electricity supply are DSOs, subcontractors, fire and rescue services, municipalities and mobile network operators. In addition, police and other authorities can be involved the situation. [1]-[10]

The main goal that DSOs have in the disturbance is to recover their operation in the network as soon as possible. Usually recovering process is planned so that the customers with biggest consumption will get the electricity back first. Regular households and summer cottages are last served. DSOs are obligated to pay so called standard compensation practise to customers in disturbances. These are stepwise increasing compensations that are paid to customer when an interruption is lasting 12 hours or longer. [1],[11],[16]

Mobile network operators are involved to disturbances of electricity supply, because there is interdependence between these two networks. Mobile network base stations need electricity to maintain their transmission. Additionally, electricity network has automation devices e.g. remote controlled switches which uses mobile network to operate. [27], [28]

The goal of the fire and rescue service is to protect people, property and environment in danger. In disturbances of electricity supply, fire and rescue service has to maintain their operation. The situation can increase the amount of their task e.g. helping people out from the elevators or clearing trees from street. Fire and rescue service has many DSOs and municipalities in their operation area. Most of the departments have divided their operation area to smaller areas, which have their own fire chiefs. Missions to rescue departments come from the local emergency call centre. [29]

Municipality has multiple duties in disturbances. They are responsible of the health of their citizens. In long lasting disturbances, municipality may have to plan an evacuation. In addition, they have home care patients that have safety buttons, which may not operate on disturbances. [1],[29]

The main goal that each actor has in disturbances varies lot. The municipality and fire and rescue service have some common in their goals; both are trying to save people, while DSO and mobile network operator are more focused on the business aspect. They want to restore their operation as soon as possible to minimize costs and compensations that they have to pay to customers.

The main problem in disturbances is that the restoration process of the DSO is concentrated highly on economic aspects and not on the aspect of the resilience of the society. At present, the legislation and standard compensation practises are directing DSO's goal to minimize the amount and duration of the disturbances. This is causing expensive measures to improve the resilience of electricity network e.g. by cabling. However, if there is a method to achieve improved resilience of the society in disturbances, it can decrease development need of the DSO. This can change the restoring order of the electricity network to more efficient way. Thus, it can help the fire and rescue service and municipality to maintain their duties in disturbances.

3 The design methods of inter-organizational situation awareness system

3.1 The design process

In this research a demonstration of inter-organizational situation awareness supply to disturbances of electricity supply has been developed. The demonstration shows how the information exchange between actors in disturbance could be improved. The development process has been iterative and methods of usability and user centred design have been used (fig 1). The research has been going already five years so the situation in the field has been changed.

Several cooperative workshops with different actors have been arranged during the development process to define the present methods in disturbances. The first version of the SA demonstration was evaluated with Nielsen's Heuristic evaluation method. Based on the evaluation the demonstration was developed further. A user need interviews were done to two fire and rescue services and one municipality. In addition, the demonstration was presented to them and questions about developing ideas were asked. Further the demonstration was improved.

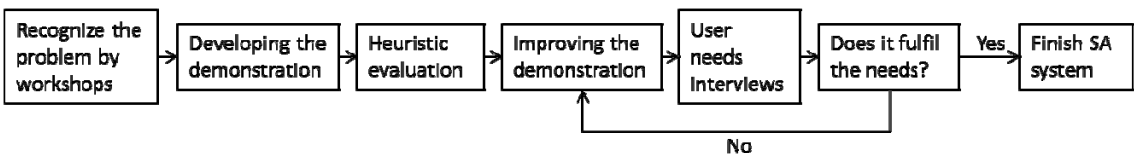


Figure 1. Iterative design process of the demonstration

3.2 Heuristic Evaluation

The heuristic evaluation was executed to our demonstration based on Nielsen's heuristic evaluation method. The meaning of the evaluation was that demonstration could be further developed into user-friendlier. Heuristic evaluation is done by observing the user interface and trying to form an opinion about good and bad parts of the user interface. The theory uses ten basic principles which been observed. Those principles are:

- Simple and natural dialogue
- Speak the user's language
- Minimize the users' memory load
- Consistency
- Feedback
- Clearly marked exits
- Shortcuts
- Good error messages
- Prevent errors
- Help and documentation

The problem of the heuristic evaluation is that individual evaluator will miss most of the usability problems in a user interface. It is recommended that there should be three to five evaluators to recognize most of the problems. [30], [31]

In this research three different evaluators observed all of the heuristic elements from the demonstration. The evaluators were three students from the Technical University of Tampere and have not been part of the developing process of the system.

3.3 User need interviews

In the interviews, the present methods achieving the situation awareness were studied. Further, it was solved what information interviewees needed to carry out their duties. The interview was semi-structured i.e. there were planned questions, but some of them were changed during the interview based on the previous answers. Further, a version about demonstration of situation awareness system was presented for the second fire and rescue department and municipality and opinion of it was asked. The demonstration was further developed based on the results of these interviews.

The interviewee from first fire and rescue service was working as an operator in their main fire and rescue department. This fire and rescue service has 22 municipalities and seven DSOs in their operating area. The respondent from the second fire and rescue department was working as a chief fire officer. This fire and rescue service has 11 municipalities and two DSOs in their operating area. From the municipality the interviewed was a leader of social services. The second fire and rescue department which was interviewed operates in the area of this municipality

The questions concerned about the usability of the demonstration and development ideas that interviewees have. Based on the answers the demonstration has been improved.

3 Situation awareness in disturbances of electricity supply

3.1 Theory of Situation Awareness

In this research, Endley's theory of three levelled situation awareness is exploited in designing the inter-organizational situation awareness system. The theory is selected because it is well known and one of the most highly cited models of SA.

According to Endsley, situation awareness (SA) can be seen as the triad of "perception", "comprehension" and "projection". In this three-level SA theory, the first level is to perceive the status, attributes and dynamics of relevant elements in the environment. At the second level the comprehension of the current situation will be created based on the information received at the first level. This means creating an understanding the meaning of the information. The third level of SA is the projection of the future about what will happen in the situation. Formation of the SA is an iterative process. During the situation new data is received and comprehension can be developed. Thus, the projection is improved. [32]-[35]

3.2 Team SA and Inter-Organizational SA

Most of the studies about the SA in the electricity network are focused on the DSO's SA. However, the disturbance situation is more complex, because there are multiple actors which have interdependencies. [34],[36],[37]

The basic theory of SA is based on individual's situation awareness and usually it is extended on the team or shared situation awareness. The team situation awareness means that every member of the team has unique situation awareness that others do not know. However, each of the members can have some awareness together. Some of the information is shared for all members and they have common awareness of that (fig. 2). In some cases there can be also different teams co-operating so that they form a team of teams. [33]-[38]

It is not clear if Endsley's theory of team SA is suitable in the case of the disturbances of electricity supply. In disturbances, different actors are forming the team of the teams. However, in Salas definition of the team, the main features of the team are that they have common goal, their specific roles are defined and they are independent [34], [37]. The problem in the case of disturbances is that the organizations hardly have any common goal. DSO's goal is to return electricity as soon as possible to minimize cost.

Fire and rescue service's goal is to safe people and property from damage. Municipality's main goal is to keep their citizens safe and confirm water and food supply. In addition, the claim of specific roles in definition does not fulfil. The

actors have specific role based on their roles in society. However, there are no established practices which would define the roles in disturbance situation.

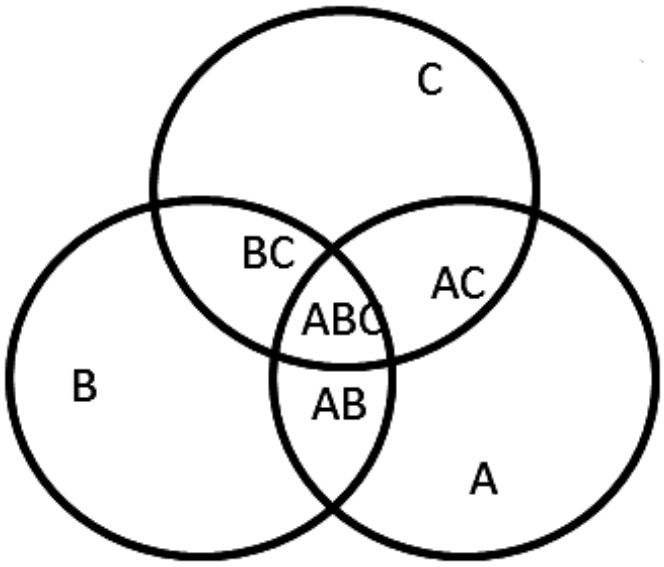


Figure 2. Team SA

As an extension to team SA theory [35] where the sub-goals have to be common in case of the inter-organizational SA the most important is that the sub-goals of different actors have an effect on each other. In the inter-organizational situations like in disturbances of the electricity supply, to find the needs of the SA, the interdependences that actors have should be detected. This way the link between the sub-goals could be found. The best example of this is DSO and mobile network operator; their networks are interdependent e.g. if the DSO restores the electricity to the important base station of the mobile network first, will they help their own restoration process by getting all remote controlled switches to operate.

The second problem with the definition of the team, specific roles, can be changed easily by increasing the co-operation between different actors. At present, some DSOs have co-operation between the fire and rescue services. In this case, they have already some common procedures.

3.3 Sources of Situation Awareness of DSO

The sources of SA of the DSO can be divided to two categories internal and external (fig. 3). At present, the information systems that DSO uses are focused mainly to internal situation awareness. These systems are Supervisory control and data acquisition (SCADA), Distribution management system (DMS), Network management system (NIS), Work management system (WMS) and Customer information system (CIS). All of these are designed to support the everyday actions of DSO. They are related to operations in electricity network like stability. [1],[29],[39]

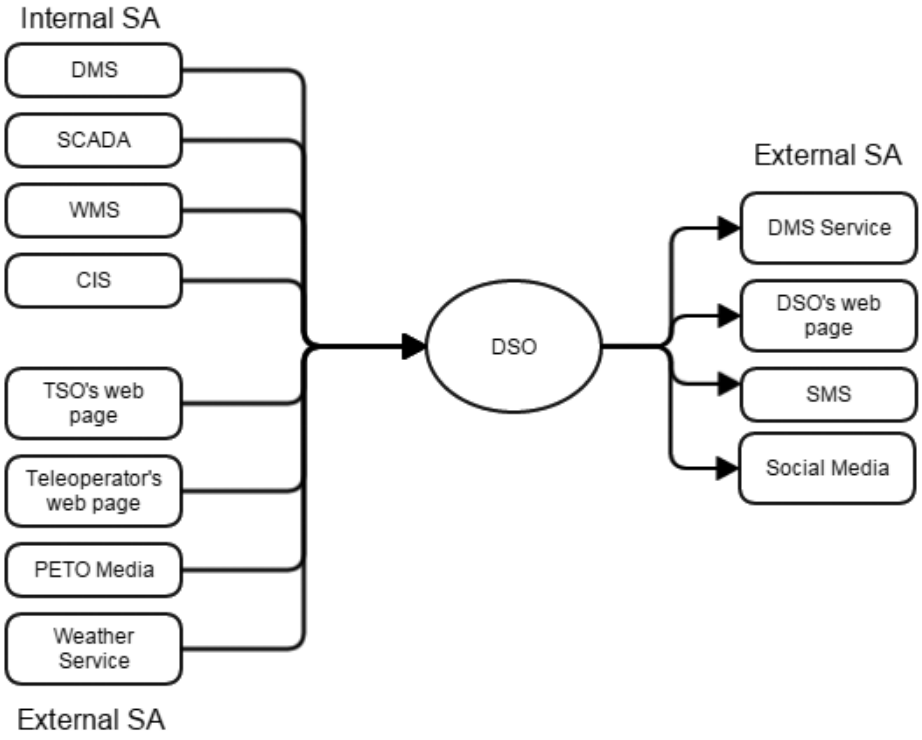


Figure 3. Sources of Internal and External SA of the DSO

SCADA collects the status and measurement data e.g. from substations. This information is used to control the network. DMS connects data from SCADA and NIS to map based user interface. With DMS the overall picture about the network can be seen. It can be used to plan and to make the reconnections in the network. At disturbance situation DMS is important tool to locate the outages and to get an overall awareness of the situation. [1],[29], [39]

In addition, the work management system is important tool in disturbances. The WMS system is used to locate the repairer teams and to communicate with them. It can be used to share tasks and send teams to right places to fix faults. [1]

The external situation awareness of DSO can be divided to information that DSO shares to other actors and customers and to information that DSO receives from others. The situation of transmission network is the main information that DSO needs, because if something happens it can affect the DSO's network. Some of the DSOs want to follow the outages of their neighbour DSOs' networks to predict if storm is coming to their operating area. However, public web pages are only way to do it. In addition to their systems DSO gets weather forecast and warnings from local meteorological institute. Other information that DSO receives can be e.g. tasks of fire and rescue services. [1]

Some DSOs are co-operating with their local mobile network operators to receive information about the location of the important base stations of mobile network. In addition, they may follow the service information of the mobile network from operator's public webpage. Some DSOs are maintaining a database about customers

that are highly dependent on electricity. However, this information is usually outdated because there are no established practices. [1],[2]

In questionnaire made at 2010 to Finish DSOs it was relieved that main means of communication with other actors in long lasting and widespread disturbance were mobile phone (96%), phone (59%) and e-mail (54.9%). Since that methods have been improved. [29]

At present, the information that DSO shares to others is focused mainly on their web pages. Most of the DSOs have a map in their web page where it can be seen where the outage is (in transformer level), when it has started, when the estimated end time is and how many customers it affects. This information comes from DSO's DMS. Some DSOs exploits DMS also to share more specific information to repairers, subcontractors and fire and rescue services. This so called DMS service is originally designed to share information to subcontractors so it is direct view from DMS. In some cases, a representative from fire and rescue service has come to DSO's operating room in disturbance to get a picture of the situation. [1],[2]

3.4 Sources of Situation Awareness of Fire and rescue service

Like in DSO's case the situation awareness of fire and rescue service in disturbance situation is focused highly on their own actions. Fire and rescue services are having information systems were they can receive tasks from emergency response centre and were they can follow their units. The fire and rescue service has to be able to maintain their duties in every condition so they are focusing that in disturbances also. [1],[29]

Few fire and rescue services have DMS service from their local DSO to follow the disturbance situation. However, most of them are still employing the public web pages that DSOs offers. Many times fire and rescue services will get first information about disturbance from the citizens, when there is tree on electricity line. In addition to DSO's systems, fire and rescue services are receiving weather forecast and warnings from local meteorological institute. [1],[29]

3.5 Sources of Situation Awareness of Municipality

Municipality's sources of internal situation awareness in disturbances consist of different databases and information systems that they have to follow their customers and citizens. Different organizations of the municipality have own systems e.g. homecare patients can be found from one system and locations of elderly people from other. These systems are not usually connected with any map, so in disturbances also map systems are needed to locate which customers are in disturbance area. [1],[29]

Municipalities do not have specific systems to follow disturbances. In most of the cases they are relying to DSO's public web pages. Some municipalities receive information about disturbances from their local fire and rescue services. That can be handled via SMS, e-mail or phone calls. [1],[29]

3.6. Problems with current methods

The common for these information systems is that they are focused mainly on level one and level two SA. These systems present information about current situation and help to achieve perception and comprehension. However, there are some problems, because the information is shattered and comes from multiple sources. This may effect on the creation of level 2 situation awareness. However, the weather forecast is supporting to have projection to future.

Another problem with present methods is that all actors are focused mainly to form an internal awareness of the situation. In addition, the information that is shared to other actors does not base on the needs of the information that others have e.g. fire and rescue services decides what information municipality could need and sent SMS about it.

The situation of the DMS service is complicated. In the interview it was found that the users do not want to use the service, because of the lacks it has. It was relieved that the service should not be related only to one DSO. Fire and rescue services operate in are of multiple DSOs, so there should be information from every DSO in their area.

In addition, it relieved that information from DMS service is not shared further to any other actors straight. Instead the information has been shared via phone calls. This could be improved with our demonstration. It enables sharing the information inter-organizationally.

One of the main problems with the DMS service was that it is designed for the constructors of DSO and not for fire and rescue service. Thus, the language it uses is very specific and the system is hard to use without training. In addition, it was found in the workshops of the research that different users need different kind of information in major disturbances e.g. fire and rescue services and municipalities.

5 Demonstration of the inter-organizational situation awareness system

5.1 Concept

The concept of the situation awareness system was developed based on co-operative workshops of the research and user needs interviews. The concept consists of real time situation awareness part and risk management that covers the development of network and preparedness. The concept can be extended to cover other critical infrastructures e.g. water supply.

In the workshops it was clarified that there is a need for information about customers who are highly dependent on electricity so called critical customers. These critical customers can be for example hospitals, home care patients, patients with respirator living at home and different critical infrastructures. The main results of the interviews were that the fire and rescue services and municipality need information from all DSOs operating in their area from simple view. It would be

necessary that there would be only one system where all relevant information could be found.

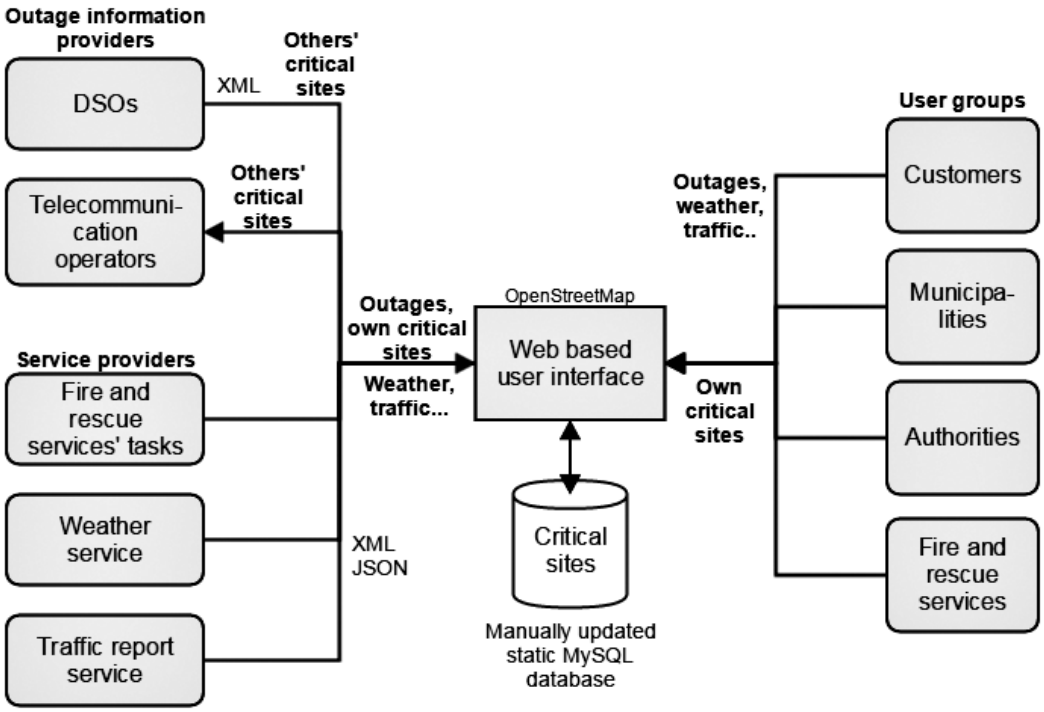


Figure 4. Concept of the inter-organizational SA system

In the concept all information related to the disturbance is gathered to one system (fig. 4). The information can be e.g. outages of electricity supply, coverage of mobile network, weather forecast and traffic reports. The main difference to existing systems is that the concept allows feed information from multiple DSOs and mobile network operators to same system.

The concept has a database to criticality information. Users can add information about their sites which are highly dependent on electricity to database. In addition to site's location, it can include information e.g. time that site can manage without electricity so called critical time and the information how bad consequences will be. The DSOs and authorities can see all the critical sites from the system. This function enables DSOs to direct restoring actions to critical sites. In addition, it helps planning the network. This database allows this system to offer level three situation awareness by presenting the information about the consequences.

To avoid information overload the system enables filtering of the information from the users' own operating area (fig 5). For example in the operating area of the municipality 1 there are two DSOs operating. Municipality can get information from the both DSOs to the same view filtered so that only outages from the area of the municipality 1 are shown.

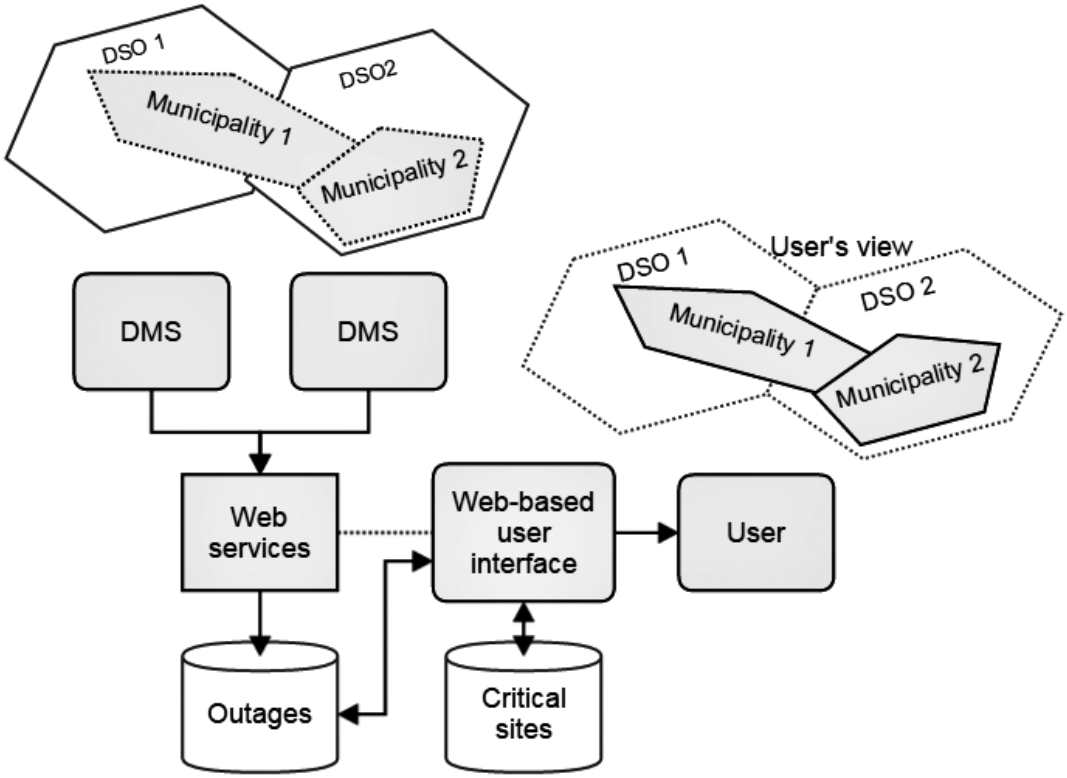


Figure 5. Municipality borderline filtering functionality [1]

5.2 The first version of the demonstration

The first version of the demonstration was built on Google Maps (Fig. 6). The demonstration presents all outages in distribution network in transformer level. Affected transformers are presented with blue lamp symbols. The system also has Google Maps' street view function which can be used to look at the environment of the site more specifically. In addition it presents critical customers that user is responsibility of. Critical customers are presented with different symbols according what is the reason of their criticality. The critical sites are shown in traffic light colours depending on what the relation of the current interruption time compared with their predefined critical interruption times.

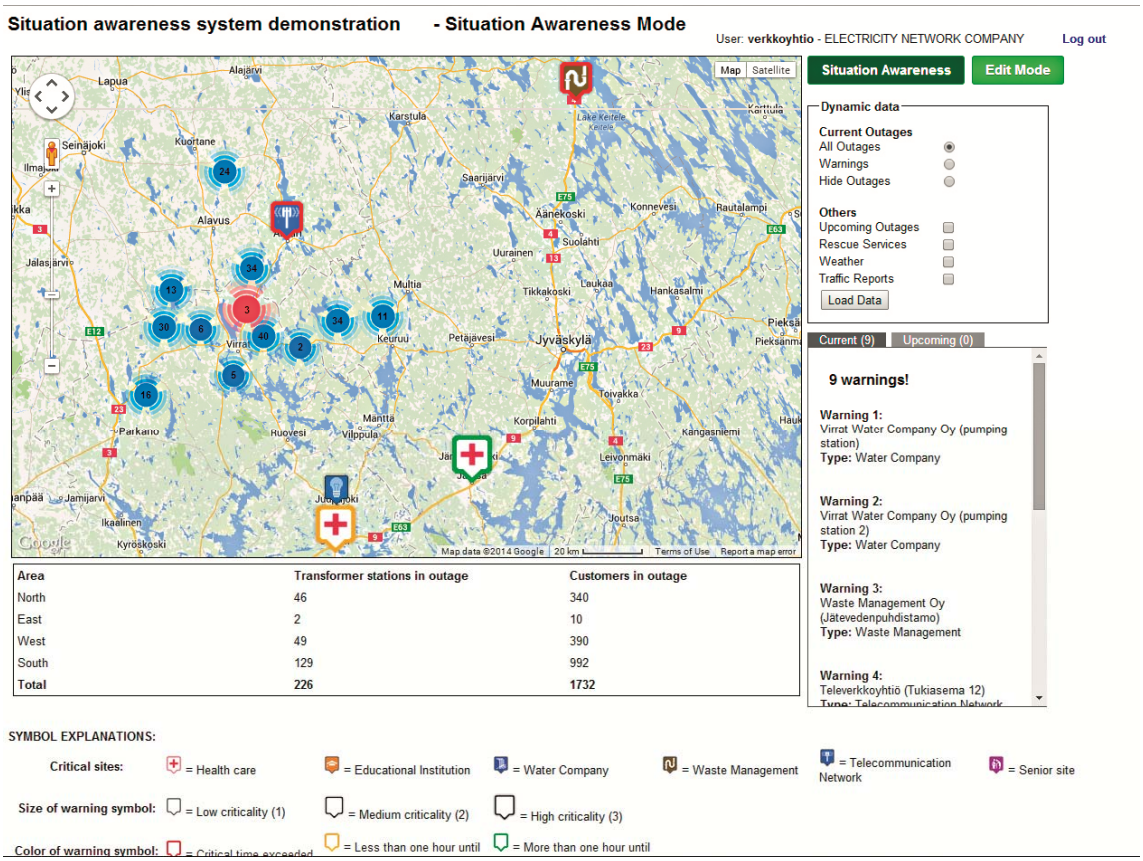


Figure 6. User interface of the first version

More information about the critical sites and the outage will appear by clicking the icons in the map. The outages are presented with blue icons in the map. Blue and red clusters in the maps combines several outages close to each other. The number in the middle of the cluster tells the number of the transformers without electricity. The colour red tells that there are critical customers in the area of outage. In addition to the map there is the table that shows amounts of secondary substations and number of the customers in outages. There is also a list of warnings where user can see information about outage and the critical sites.

5.3 Results of the heuristic evaluation

As a result of the heuristic evaluation it was notices that in principle of simple and natural dialogue the demonstration has a simple view which is easy to handle by glancing. The view is light and easy to picture. There are only three main elements the map, the table and the warnings, which clarify the view. The most important element in the system, the map, dominates the view and is easy to notice. Using the clusters to combine outages next to each other minimizes the information brought to the user. Colours used to show the critical time are a clear way to express the criticality. However, if user is taking black and white hardcopy meaning of these colours disappears. This can be problem also for colour blind persons.

There are problems with that boxes it uses are different in comparison with each other. When choosing the viewed page, buttons “Situation Awareness” and “Edit Mode” are presented with similar forms and different green colour and thus it is

hard to notice in which mode you are. Problems continue with the fact that all information does not fit into one view. It is complicated when user has to scroll the view in a different direction. Furthermore, the appearance of the demonstration is unfinished and the explanation of the symbols takes too much space. The appearance could be finished by adding softer colours and rounding the corners. The colours or the form of the page buttons could be defined better that it would be clear in which page you are.

Terminology used in the system is quite specific professional terminology. However, it is easy to understand even if user is not a specialist. Symbols of the demonstration are simple and commonly known for example a red cross symbol for a hospital. The ways to present the criticality of the sites, by the size of the symbol and the state of the critical time, with traffic lights, are clear. In addition, the system uses radio buttons to add information to map, which is common way.

Minimizing the users' memory load is fulfilled by using common ways to login. User group "Authorities" does not have to give any input while using the user interface. Choosing the views that user want is easy by clicking boxes nearby the map. These all help to minimize the memory load, because user does not have to remember any commands. The user interface does not need specific studying, it easy to learn by trying different elements of the system. The elements that can be clicked are presented so that they can be recognized to be dynamic. Using the system is every time similar, because the elements are all staying in their places. User does not have to remember anything or focus when using the user interface. Continuing the use of the system after distractions is simple. All symbols are explained under the map, so the user does not have to remember them.

Consistency in the system is great. The outage information is presented clearly, because only the customers who are shown are those without the electricity. Google Maps is very familiar to users and markers in the system works similarly than in Google Maps. The logout button is in the upper right corner which is a common place for it, so it is easy to locate. Different elements of the system are gathered to boxes so that there is on subject always in the same box. The problem with consistency is that "Situation Awareness" and "Edit Mode" buttons are presented with strong colours. It makes them dominate the view and user may think that they are more important element than they are meant to be. In addition, the tables under the map look different in "Situation Mode" and "Edit Mode". There are consistency problems with info windows, some of them disappear when clicking them and some when mouse is not at top of the icon. In addition, in "Edit Mode" the info window has scrolling part in it. The user interface does not use any sound elements. Some voice signal to warn user when critical time is achieved could be added. However, in some using environment there maybe already too many voices, it could just increase the distraction of the user. The user interface works like related map based systems and that add consistency to it. The main problem with consistency in the system is that it does not work well with every internet browser. Some functions look different and some do not work at all when using different browsers.

There is lack in feedback in the system. Map updates quite rarely and it is hard to notice if it has already updated. There should be some kind of feedback to user when updating has happened. However, new information uploads quickly when user changes something in the view.

Clearly marked exits are executed well in the system. Moving between different views is handled with buttons "Situation Awareness" and "Edit Mode". Otherwise there is no need for exit any views. Different views of the map are easy to change by clicking boxes next to the map. Logout is placed clearly. However, it could be marked as a button and not a link like it is now.

Shortcuts are executed so that there is possibility to hide symbol explanations. However, it is not marked clearly. In the map there are chances to zoom with mouse scrolling or with the zoom marks in the map. There is no possibility to personalize the view. When there are multiple organizations using the system, they may want to highlight different elements of the system. While login, the cursor is not located to the text box. It should be changed so that it would be already in the first box.

One of the observed things was error messages. They are executed clearly in the system. If a user uses wrong user identification, the error message tells why login did not work. However, the place of the error messages could be on the upper side of the login textboxes. Now it is executed so, that there comes a new error page and you have to go back to the previous page to try to login again. These are the only error messages in the system. There could be also some error message if the update fails with the possibility to inform the administrator. In addition, error message about using the wrong internet browser could be provided.

Prevent errors is fulfilled so that there are no chances to get the system stuck by using it wrongly. If user makes mistakes with the input of the user identification, it is not possible to continue before giving the right information. The user interface is so easy to use that the possibility of errors is small even without reading the directions or in problem situations.

Because the system is still a demonstration there is no documentation with directions. The system does not give any instructions at all while using it. This part of observed things has not been fulfilled well. However, there is explanation for all symbols that map uses in bottom of the page and the system is quite easy to use even without manual.

The results of the heuristic evaluation were that the demonstration has a clear user interface and it is easy to use even without a manual or training. In addition, the system does not add much memory load on user, and the terminology is easy to understand. Further, the consistency is good at overall even there are some minor consistency problems. The evaluation reveals that there are still multiple lacks in the development of the demonstration e.g. there is no manual and there is lack of the error messages. However, most of these problems indicate only that the system is still under the development process. Thus, those can be fixed later on.

5.4 Version 2 of the demonstration

Based on the heuristic evaluation, the user interface was cleaned and harmonised. Further, the map was changed to open source. The user interface was fitted to screen size, so there is no need to scroll. The view was made softer by removing the box frames.

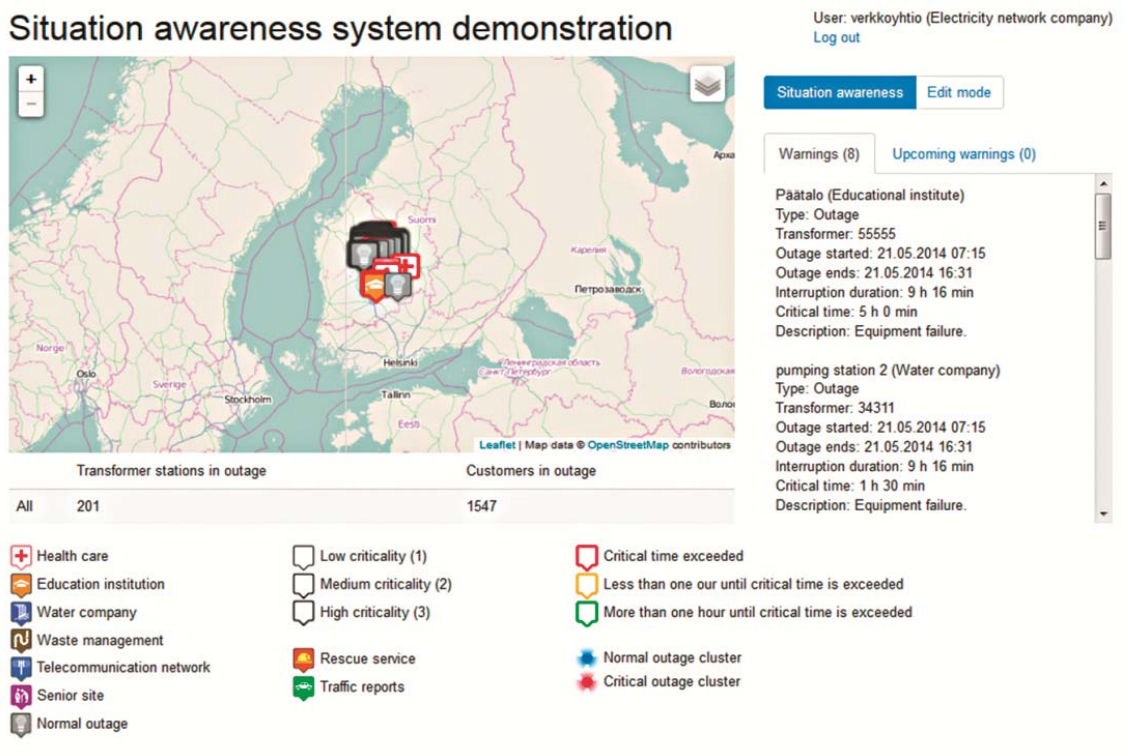


Figure 7. User interface of the second version

The main new character was the municipality borderlines added on the map (Fig. 8). These lines help municipalities and fire and rescue services to observe their operating area.

5.5 The results of the user need interviews

In the interviews, the response to the demonstration is mainly positive. Especially the municipality thinks that situation awareness system would highly improve their operability in disturbances. The functionality to add critical sites is appreciated.

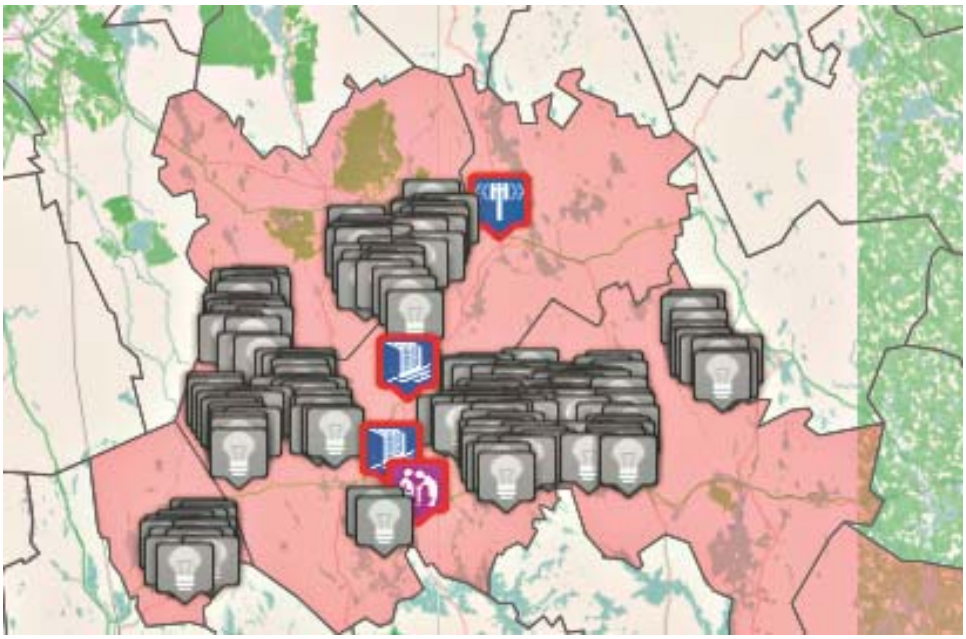


Figure 8. New municipality borderline functionality

The main results of the interviews were that the information needed varies a lot depending on the actor. The main needs are listed here:

Municipalities need to know:

Are there home care patients or elderly people in disturbance area?

Is there a disturbance of electricity supply or mobile network in their operation area or in neighbor municipalities?

Do the residents need help to get food, water or shelter?

Are there patients with safety phones or safety buttons that do not have electricity or mobile network?

What is the weather forecast?

Fire and rescue services need to know:

Are people in danger?

Is there disturbance of electricity supply mobile network in their operation area?

Is there need for evacuation by municipality?

What is the weather forecast?

At present systems, fire and rescue services are not able to send any information back to DSOs. Thus, the main need that the all interviewees have is bidirectional

functions to SA systems e.g. units of fire and rescue service would like to inform DSO if they see a tree on power lines. They are not allowed to do anything for those, which is why it would be good to have a system where they could mark the fault places that they have seen and sent it to DSOs.

The municipality desires information layers that can be activated and deactivated easily. The main need is for layers of location of all elderly citizens and disabled people. The information about their outages can help municipality to target their evacuation and so improve their resilience.

In addition, the fire and rescue service often needs information about which DSO is operating in which address. This could be solved with automatically finding service in the system, where the user could write the address or connect geographical information to the system and would receive information about operating DSO. This kind of service has not been executed in any of the present systems studied in the research.

All interviewees think that the information about planned outages is unnecessary because in the case of the planned outages, the sites are informed beforehand and are prepared.

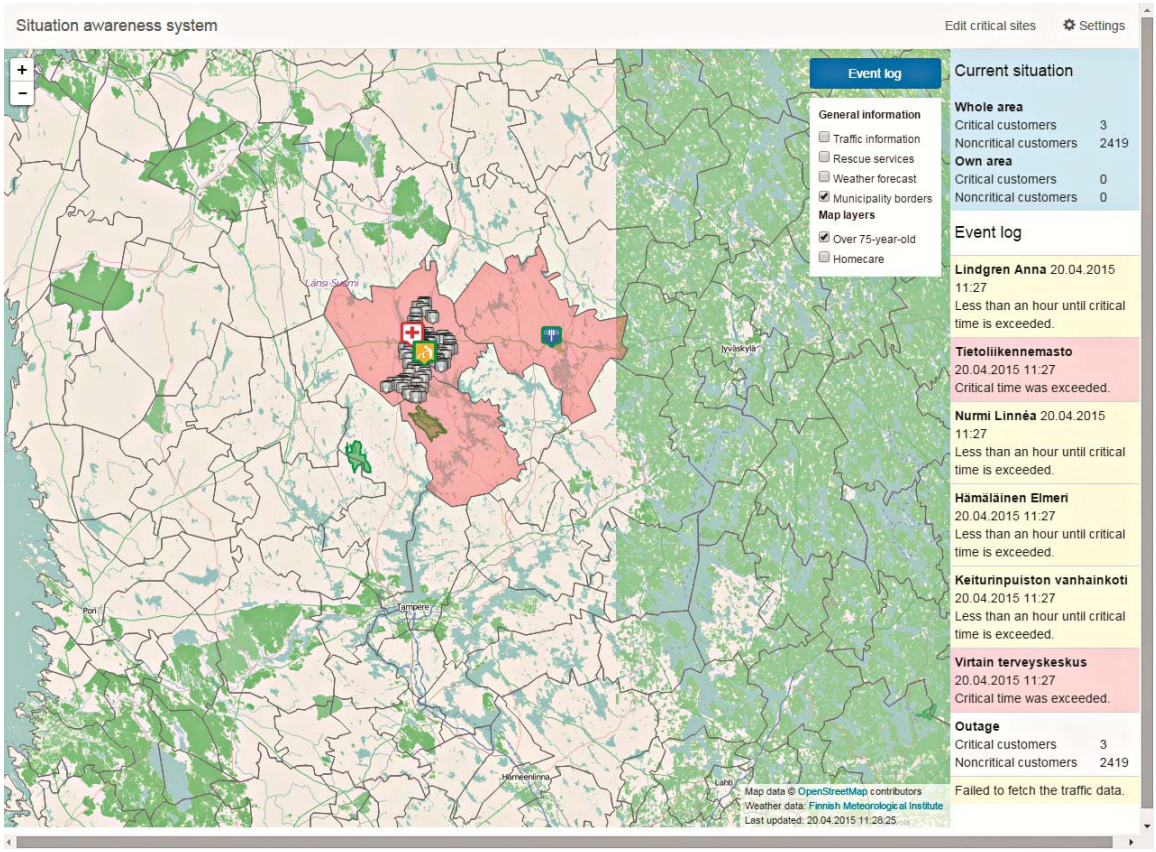


Figure 9. Improved user interface of the latest version

4.4 The latest version of the demonstration

Based on the results of the interviews the new version of the demonstration has a larger map view (fig 9). This version automatically filters the information to right operating area. However, user can change the filtering whenever it is necessary. In this version, the user can define what layers they desire when they are implementing the system. There is a menu on the upper right corner of the map where activation and deactivation of the layers is easy to carry out. To improve the visibility of the critical sites the size of transformer symbols is decreased to smaller and colour changed to grey.

The main target of the development has been to improve the simplicity of the user interface. All interviewees were concerned that the system has to be simple enough because it is used in extreme situations.

The view is personalized according the needs of information that user groups have. The personalization is made to reduce unnecessary information. There are information layers that user can add to map when the extra information is needed (e.g. municipality can choose a layer of all citizen older than 70 years) (fig. 10). The user can filter the map to show only their operating area to avoid information overload.

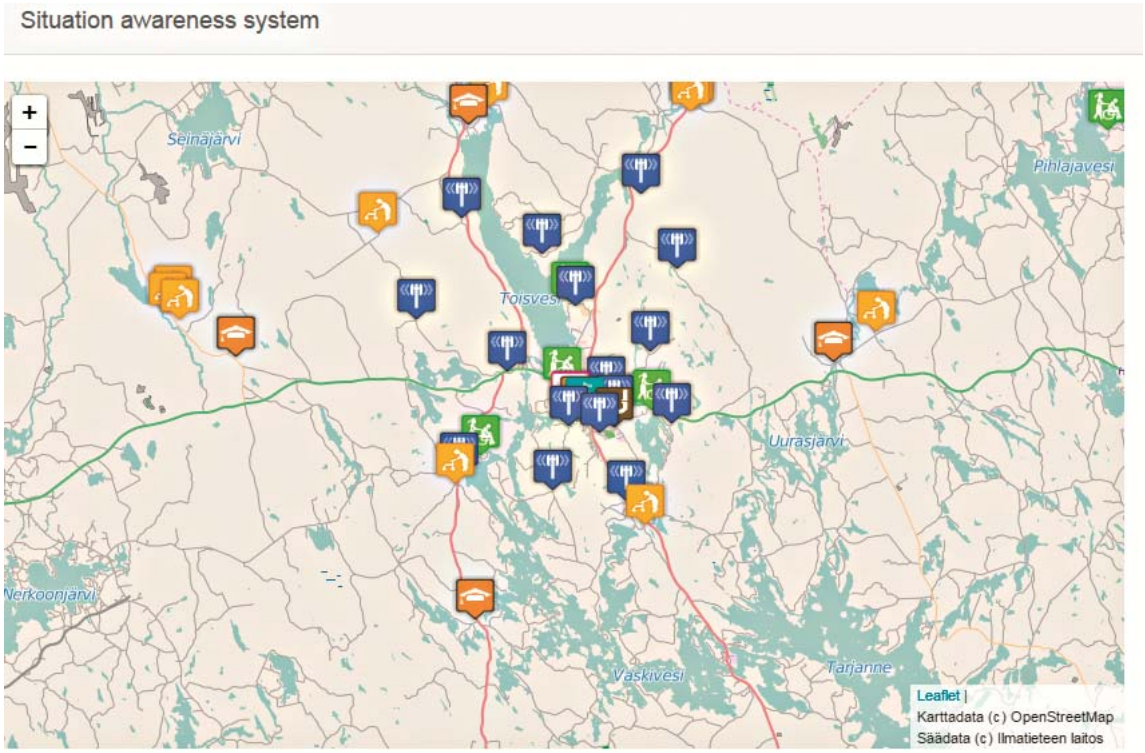


Figure 10. Closer look of the user interface

The level of criticality is presented with different sizes e.g. central hospital has a bigger symbol than local health centre. The situation has been presented with traffic coloured frames in symbol. This colouring system helps user to predict what can happen in future e.g. municipality can arrange an evacuation to critical customer if it

seems that the outage is lasting longer than the critical time. In addition it helps DSO to plan the restoration order.

In addition to map there is event log next to it. Event log will give information about amount of normal and critical customers that do not have electricity. This information can be used to get an overall picture of situation. However, to get more precise information there are warning messages that alarms if the specified critical time of critical customer is going to exceed. These warnings are marked with traffic light colours.

The latest functionality in the demonstration is information about mobile network coverage shown in figure 11 (the map layer has been removed because of confidentiality clause). This information comes from mobile operators system and is processed to layer on map. This information can be processed so that user sees only areas that do not have any mobile coverage. In addition, it can be processed so that it presents all coverage including those which functions still and those which comes from the base station which working on back up battery.

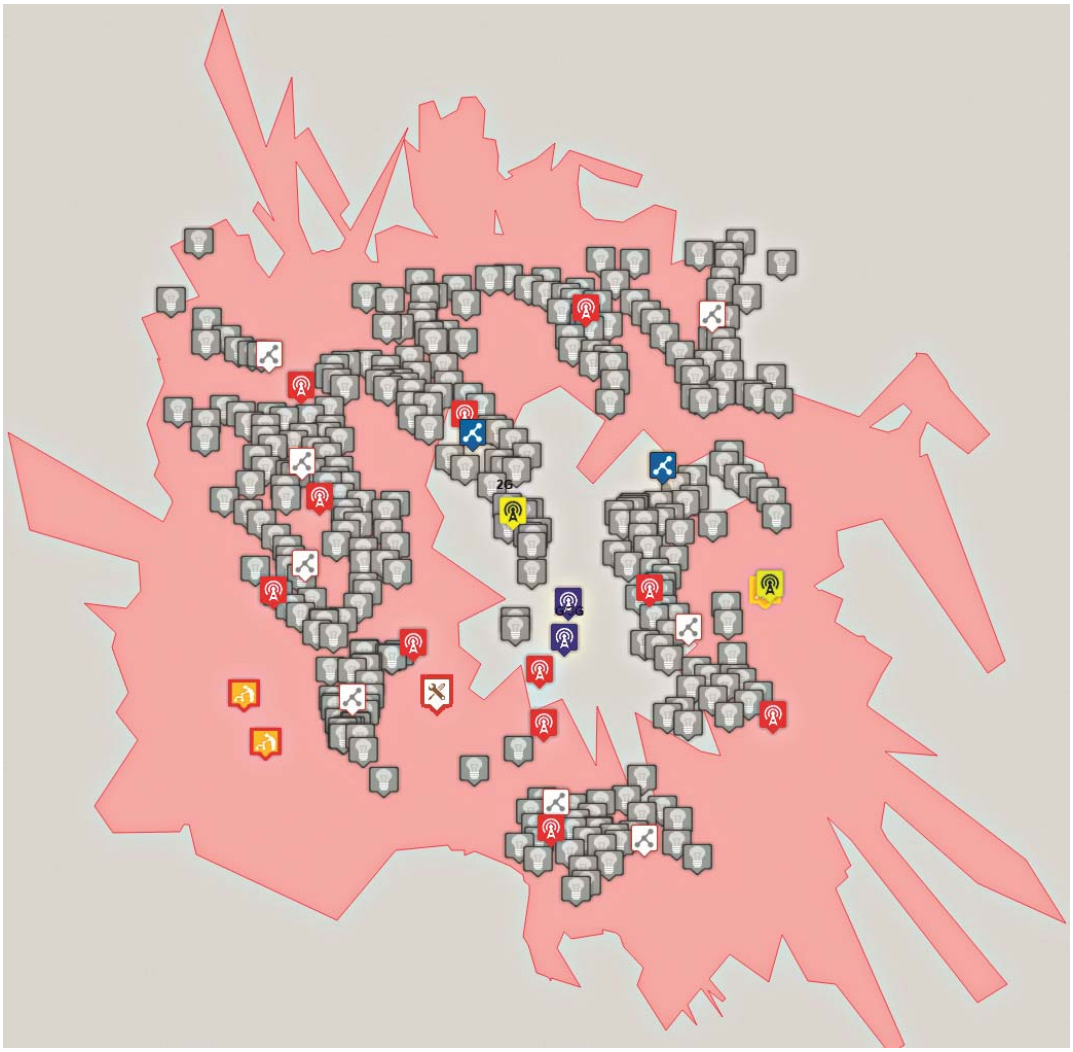


Figure 11. Coverage of the mobile network functionality

This functionality can be useful e.g. to municipalities to find if there are safety button users who do not have mobile connection. In addition, DSO can utilize the functionality to observe if they have remote controlled switches on the area without coverage. This information can be useful for DSO when they will make projection about future. Thus, it can be utilized to warn the repair team that the communication with control room operator will be vanished.

5 Further studies

The demonstration of the situation awareness system has not been in live testing yet. The next step of this research is to test the demonstration in real life use. It will be implemented on two DSO's operating room, to one municipality and fire and rescue service. With this life testing it is possible to achieve more knowledge how the inter-organizational situation awareness system could improve the resilience of society in disturbances.

In testing process, different measurement methods can be utilized to detect the level of SA and work load of the system e.g. Nasa TLX, freeze tests and Situation Awareness Global Assessment Technique (SAGAT). The results of the test can be utilized to improve the system and to develop the demonstration to real system.

Conclusion

Disturbances of electricity supply are complex situations with multiple actors. All actors have own goals based on the legislation and responsible they have. There have been problems in information exchange between these actors. The sources of the situation awareness in disturbance is shattered and designed mainly on purpose of internal situation awareness.

The theory of team SA has to be extended to cover inter-organizational situations where the goals of the actors are more like linked to each other than common. Disturbances of electricity supply are good example of this. The sub-goals that actors have in disturbances are affecting to each other. These links can be found by studying the interdependences of the actors.

In this research it clarified that the present restoration process of the electricity network causes problems to information exchange. The legislation and standard compensations are directing DSO's goal to minimize the amount and duration of the disturbances. However, the inter-organizational situation awareness system could improve the resilience of the society in disturbances, thus decrease development need of the DSO. This can change the restoring order of the electricity network to more efficient way.

A demonstration of inter-organizational situation awareness system has been developed, in this research. The design process has been iterative and needs of the different actors have been acknowledged. Comparing to existing sources of SA in disturbances the system can provide information from multiple actors to one view. In addition, the demonstration supports level three situation awareness by traffic light colouring system and warnings.

In the demonstration, the view is personalized and the information is filtered. This is improvement for present ways to information exchange like DMS service that gives too detailed technical information to fire and rescue service.

The design process of the demonstration has to continue to achieve the optimal situation awareness in disturbances. Testing in live situations should be arranged to detect its work load, usability and capability to support the SA.

References

[1] "Demonstration of the Inter-Organizational Situation Awareness System to Major Disturbances". CIRED 23rd International Conference on Electricity Distribution. 15.-18.6.2015. Lyon, France.

[2] Krohns-Välimäki H., Aalto H., Pylkkänen K., Strandén J., Verho P., Sarsama J., 2014. "Developing Situation Awareness in Major Disturbances of Electricity Supply". IEEE PES Innovative Smart Grid Technologies, Europe (ISGT EU). 12.-15.2014. Istanbul, Turkey.

[3] Krohns-Välimäki H., Strandén J., Pylkkänen K., Hälvä V., Verho P., Sarsama J., 2013. "Improving shared situation awareness in disturbance management". CIRED 22nd International Conference on Electricity Distribution. 10.-13.6.2013. Stockholm, Sweden.

[4] Krohns H., Hälvä V., Strandén J., Verho P., Sarsama J., 2011. "Demonstration of Communication Application for Major Disturbances in the Supply of Electric Power". CIGRE International Symposium – The Electric Power System of the Future. 13.-15.9.2011. Bologna, Italy.

[5] J. Strandén, V.-P. Nurmi, P. Verho, M. Marttila, "State of preparedness of Finnish Society for Major Disturbance in Distribution of Electricity.", International Review of Electrical Engineering [I.R.E.E.] vol. 4, n. 2, pp. 211-219, Apr. 2009

[6] J. Strandén, H. Krohns, P. Verho, J. Sarsama, "Major Disturbances – Development of Preparedness in Finland During the Last Decade.", 21st International Conference on Electricity Distribution (CIRED 2011). 6.-9.6.2011. Frankfurt, Germany.

[7] Energy Market Authority, "Summer 2010 storms in point of view of electricity grid" ["Kesän 2010 myrskyt sähköverkon kannalta" in F innish]. Report, 306/401/2011, Finland 2011

[8] Con Edison Media Relations, "Con Edison restores 225,000 customers", News 1.11.2012, [Online] Available: http://www.coned.com/newsroom/news/pr20121101.asp

[9] Union for the Coordination of Transmission of Electricity (UCTE), "Final Report – System Disturbance on 4 November 2006.", January 2007. [Online]. Available: http://www.ucte.org/_library/otherreports/Final-Report-20070130.pdf

[10] U.S.-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendation", U.S. Department of Energy, Report 2004, [Online]. Available: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

[11] The Finnish Electricity Market Act 588/2013.

[12] Ley B., Pipek V., Reuter C., Wiedenhoefer T., "Supporting Inter-Organizational Situation Assessment in Crisis Management", Proceedings of the 9th International ISCRAM Conference 2012

[13] Schweer A., Schaum K., Hollmach D., "A New grid driven approach to guarantee reliable communication during power outages", in Proc. 22nd International Conference on Electricity Distribution (CIRED 2013)

[14] Lakervi, E. & Partanen, J. 2008. Sähkönjakelutekniikka [Distribution system automation; In Finnish]. Otatieto, Helsinki

[15] Finnish Energy Industries. 2014. Keskeytystilasto 2014 [Interruption statistics 2014; in Finnish].

[16] Strandén J., Krohns-Välimäki H., Verho P., Sarsama J., Hälvä V., 2014. "Influence of Major Disturbances in Electricity Supply on the Operating Environment of Distribution System Operators: a Case Study". International Review of Electrical Engineering (IREE). Vol 9., No 2, pp. 363-372

[17] Sener and Finergy, 2002. "Senerin ja Finergyn myrskykyselyiden yhteistuloksia" [Summary of storm questionnaire by Sener and Finergy; in Finnish], Finland

[18] Forstén J., 2002. "Sähkön toimitusvarmuuden parantaminen" [Improving the reliability of electricity supply; in Finnish], The Ministry of Trade and Industry, Helsinki, Finland

[19] Landstedt J., Holmström P., 2007. "Electric power systems blackouts and the rescue services: the case of Finland," Emergency Services College of Finland and State Provincial Office of Western Finland, Helsinki, Finland, Working Paper 2007:1 of CIVPRO (Civil Protection Network).

[20] Finnish Energy Market Authority, 2011. "Kesän 2010 myrskyt sähköverkon kannalta" [Summer 2010 storms from the electric power network point of view ; in Finnish], Helsinki, Finland.

[21] Accident Investigation Board of Finland, 2011. "Heinä-elokuun rajuilmat" [The storms of July-August 2010; in Finnish, abstract in English], Helsinki, Finland.

[22] Finnish Energy Industries. 2012. "Loppuvuoden katkoista kärsi 570 000 asiakasta" [570,000 customers suffer from the interruptions experienced at the end of the year; in Finnish]. [Online]. Available: http://www.energia.fi/ajankohtaista/lehdistotiedotteet/loppuvuoden-sahkokatkoista-karsi-570-000-asiakasta

[23] M. Peltonen et al., 2003. "Metsätuhotyöryhmä" [Forest damage working group; in Finnish], Ministry of Agriculture and Forestry, Helsinki, Finland, Memorandum 2003:11, May 30, 2003.

[24] Finnish Energy Industries, 2012. "Lausunto työ- ja elinkeinoministeriön ehdotukseen toimenpiteistä sähkönjakelun varmuuden parantamiseksi sekä sähkökatkojen vaikutusten lieventämiseksi" [Comments for the proposal of the Ministry of Employment and the Economy for measures of improving reliability of electricity supply and mitigating consequences of power outages; in Finnish], Helsinki, Finland, Apr. 24, 2012.

[25] Ministry of Agriculture and Forestry. 2011. "Myrskyissä kaatui puita noin 120 miljoonan euron arvosta" [Storms cut down trees worth 120 million euros; in Finnish]. [Online]. Available: http://www.mmm.fi/fi/index/etusivu/tiedotteet/myrskyissakaatuipuitanoin120miljoonaneuronarvosta.html

[26] Federation of Finnish Financial Services. 2012. "Tapani- ja Hannu-myrskyjen korvaukset täsmentyivät yli 100 miljoonaan euroon" [Compensations for the Tapani and Hannu storms were specified at over 100 million euros; in Finnish]. [Online]. Available: http://www.fkl.fi/ajankohtaista/tiedotteet/Sivut/Tapani-ja-Hannu.aspx

[27] Horsmanheimo S., Maskey N., Tuomimäki L., Kokkoniemi-Tarkkanen H., Savolainen P., 2013. "Evaluation of Interdependencies between Mobile Communication and Electricity Distribution Networks in Fault Scenarios". Innovative Smart Grid Technologies Asia 2013 (ISGT Asia 2013). 10.-13.11.2013. Bangalore, India.

[28] Hyvärinen M., Pettisalo S., Trygg P., Malmberg K., Holmlund J., Kumpulainen L., 2009. "A Comprehensive Secondary Substation Monitoring System". 20th International Conference on Electricity Distribution (CIRED 2009). 8.-11.6.2009, Prague, Czech Republic.

[29] Krohns H., Strandén J., Verho P., Sarsama J., 2010. "Developing communication between actors in major electricity distribution network disturbances". Nordic Electricity Distribution and Asset Management Conference 2010. 6.-7.9.2010. Aalborg, Denmark.

[30] J. Nielsen, R. Molich, "Heuristic evaluation of user interfaces", CHI '90 Proc. of the SIGCHI Conference on Human Factors in Computing Systems, pp. 249-256

[31] J. Nielsen, "Usability engineering", vol. 1. San Francisco: Academic Press, 1993, pp. 115-163

[32] Endsley M.R,. 1995. "Toward a Theory of Situation Awareness in Dynamic Systems". Human factors, vol. 37, pp. 32-64

[33] Endsley M.R., Connors E.S. 2008. "Situation Awareness: State of the Art", in Proc. 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century

[34] Endsley M.R., 2015. "Situation Awareness Misconceptions and Misunderstandings". Journal of Cognitive Engineering and Decision Making March 2015 vol. 9 no. 1 4-32

[35] Endsley M.R., Jones D.G., 2011. "Situation Awareness: An approach to User-Centered Design" Second edition. CRC Press pp. 193-218

[36] Panteli M., Crossley P.A., Kirschen D.S., Sobajic D.J., 2013. "Assessing the Impact of Insufficient Situation Awareness on Power System Operation". IEEE Transactions on power systems, vol. 28, No. 3 pp. 2967-2977

[37] Panteli M., Kirschen D.S. 2015. "Situation awareness in power systems: Theory, challenges and applications". Electric Power System Research, Elsevier, May 2015, Vol. 122, pp. 140-151.

[38] Nofi A. A, 2000, "Defining and Measuring Shared Situational Awareness", Report, Center of Naval Analyses, Virginia

[39] Northcote-Green, J., Wilson, R. 2006. "Control and Automation of Electrical Power Distribution Systems". CRC Press. pp. 31-60.

Principles of designing for situation awareness

Jussi Haapanen
Tampere University of Technology
jussi.haapanen@tut.fi

Abstract

High level of situation awareness is a key factor in many domains to ensure correct decision making and actions. Situation awareness has been studied extensively in the aviation and military domains but the research also applies to other domains e.g. power grid operations and managing disturbances of electricity supply. Based on the research design principles have been created in order to help system designers to create better user interfaces for systems used in operational activities. These principles have been applied when designing the situation awareness system concept for managing disturbances of electricity supply.

Purpose

The purpose of this article is to present the theory of situation awareness, how to design for situation awareness and how the design principles have been applied to a situation awareness system concept for managing disturbances of electricity supply.

Keywords

Situation awareness, disturbances of electricity supply

Paper type

Project work for the post-graduate course at National Defence University.

1 Introduction

Situation awareness is a concept used in many domains ranging from surgery operation to power grid operation and aviation. It has been studied and used extensively in the aviation and military domains but it applies to any domain with operational activity. Situation awareness can be traced to the 1st World War where the military aircraft crews recognized it as an important component for successful operation. The term situation awareness was first used by the United States Air Force fighter crews after returning from the war in Korea and Vietnam. High level of situation awareness was identified as a decisive factor in air combat. Situation awareness during operation is crucial for the operator in order to make correct decisions and carry out correct actions.

Situation awareness can be supported by systems used by the operator during operation. It is also possible for a system to degrade the operator's situation awareness by providing information in an incorrect way. Due to this the support for situation awareness should be taken into account when designing systems for

operators. The systems designed in the aviation domain have long utilized the principles and best practises defined in the research but in some fields such as the power grid operations the situation awareness as a concept has only recently aroused interest.

In this paper a demonstration of situation awareness system for managing disturbances of electricity supply is presented. In addition the user interface design choices for the system are explained in the paper. The Mica R. Endsley's theory of situation awareness is discussed in chapter 2. The design principles defined by Endsley are presented and discussed in chapter 3. The designed situation awareness system concept and it's user interface components are discussed in chapter 4.

2 Situation awareness

Having a high level of situation awareness means being aware of what is happening around you and understand what the information means to you currently and in the future. The concept of situation awareness is applied to operational situations such as aviation and power grid operation, where an operator has to have situation awareness in order to perform actions correctly (e.g. in order to separate traffic as an air traffic controller or operator power grid as a power grid operator). In such situations only the information relevant to the current task is important for situation awareness. For example in power grid operations the operator does not have to know the age of the network components in order to operate the power grid. Instead he must be aware of the current load flows and the status of different grid components. [1]

There are multiple models for describing situation awareness. A commonly used model was defined in [2]. In Endsley's model situation awareness is formally defined as

"The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future."

Other models such as the perceptual cycle model [3] and the activity theory model [4] exist but these are not discussed in this paper.
Endsley [1] divides situation awareness into three levels:

Level 1–perception of the elements in the environment
Level 2–comprehension of the current situation
Level 3–projection of future status

These levels are discussed more in the following sub-chapters. Each level of situation awareness is important in order to have an extensive awareness of the situation. The model has been criticized by saying that it states that the next level situation awareness cannot be achieved without achieving the previous level situation awareness [5]. According to Endsley, this is a misunderstanding of the model. The user does not need the previous level of situation awareness to achieve

higher levels of situation awareness the user still needs them to achieve an extensive awareness of the situation. [6]

2.1 Level 1–perception of the elements in the environment

In order to achieve any sort of situation awareness the operator must perceive the status, attributes and dynamics of relevant elements in the area. The information can be perceived through different senses such as visual, auditory, tactile, taste or olfactory senses. [1] For example in power grid operation the level 1 situation awareness consists of information like planned outages, load forecast, reserves and switch/breaker statuses.

Perception of the information can be difficult. There are multiple reasons why an operator fails to perceive information. The operator has to be vigilant at all times.
If the operator is not vigilant enough, it is likely that critical information will be missed. Perception of information can fail because of too much automation. Too much automation causes the operator so called "out-of-the-loop"-syndrome in which the operator does not know what is going in the system. Other operator-independent reasons can also cause the operator to miss critical information. For example in power grid operation there can also be issues with the devices measuring the necessary variables. If the measurement devices fail to measure the variables correctly due to a fault in the device, it is possible that the operator performs actions incorrectly because of incorrect information. Another possible issue is if the telecommunication network fails to deliver the measurement data to the control center. In such cases it is possible that the operator is unaware of the network state and fails to make correct decisions in the operation. [7] In addition in the power grid operation the power grid is not the only subject the operator has to be aware of. The operator has to also be aware of the status of telecommunication networks, which can be difficult as the telecommunication networks are often operated by other companies and information exchange between actors is low. If the operator is unaware of the telecommunication network fault, it is likely that a lot of time will be wasted trying to send control commands to power grid devices instead of manually operating them. [8]

Jones & Endsley [9] discovered that 76 % of pilots' situation awareness errors occurred because of pilots not perceiving the information needed. Around 40 % of these errors occurred because the needed information was not provided to the person needing it or was not provided clearly due to system limitations or shortcomings. For example the runway lines had become faded and obscured. In approximately 30% of the cases the information was presented but was not perceived due to too high a workload or outside distractions such as a phone call. In some cases the operator did not bring up a view where the needed information was presented.

In power grid operation the workload is often an issue in the major disturbances of electricity supply. There can be hundreds of alerts on the displays and operators have to coordinate the fixing with the repair crews. In such situations it is also likely that in addition to the operators there can be multiple people in the control center

such as a contact person from the rescue services, members of the media and other personnel causing the level of noise increase, making focusing harder which in turn makes forming high level of situation awareness difficult. [10]

2.2 Level 2-comprehension of the current situation

Having a good level 2 situation awareness means that the operator understands what the perceived information means for the operation. Level 2 situation awareness is formed by connecting level 1 situation awareness data with the operator's goals. Information is prioritized based on the operator's current goals. A good analogy for level 2 situation awareness is having a high level of reading comprehension as opposed to just reading words. In power grid operation the level 2 situation awareness consists of things like understanding the deviation between actual and planned states, the status of equipment, the capabilities and vulnerabilities of the system and available actions. If and operator does not understand what certain actions can do based on the current network state, the operator can execute incorrect actions and accidentally cause a blackout. [7]

According to Jones & Endsley [9] around 19 % of situation awareness errors in aviation were caused by problems in level 2 situation awareness. In the cases the operators are able to perceive the necessary data but cannot understand the meaning of the information. For example a pilot understands that the altitude of the aircraft is 3 000 meters but do not understand that he had deviated from the level assigned by the air control.

2.3 Level 3-projection of future status

Level 3 situation awareness means the operator's ability project future status of the situation. In order to properly project the future, the user must have perceived and understood the current status. User can create projections without level 1 or level 2 situation awareness but the accuracy of the projections will be higher with more extensive level 1 and 2 situation awareness. For example pilots and air traffic controllers actively project the movements of other aircraft in order to prevent problems. [6] In power grid operation level 3 situation awareness means being able to project things like future system state and the time when to implement actions. [7]

Only 6 % of errors in situation awareness occurred because of lacking level 3 situation awareness. These errors are often caused by over projecting current trends. The amount of situation awareness errors because of lacking level 3 situation awareness is low because most of the errors occur in level 1 and 2 situation awareness. [9]

2.4 Team and shared situation awareness

In many complex domains such as aviation, military operations and managing disturbances in electricity supply it is often necessary for people to work together in order to achieve a common goal. Team and shared situation awareness are important concepts in such domains. The team and shared situation awareness can be seen in figure 1.

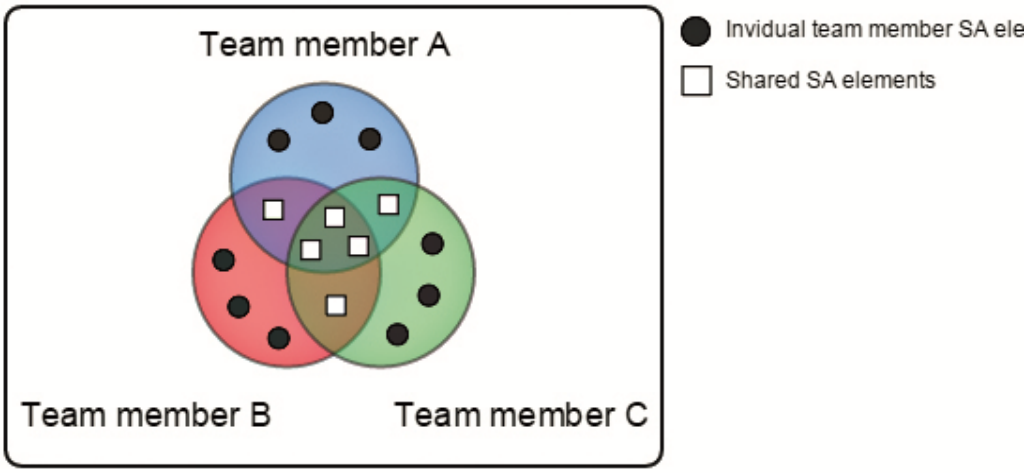


Figure 1. Team and shared situation awareness. [11]

Endsley [1] defines team situation awareness as

”the degree to which every team member possesses the SA required for his or her responsibilities”

and shared situation awareness as

“the degree to which team members have the same situation awareness on shared situation awareness requirements”.

Basically shared situation awareness can be seen in the middle of the figure 1 where the invidual actors’ situation awareness overlaps. Good team situation awareness on the other hand means the situation awareness of each actor should be at high level for the team to succeed in completing the goals. In the figure 1 this means that the dark circles (each team members situation awareness) should be at high level.

Panteli [11] lists the requirements for each level of shared situation awareness. The requirements can be seen in table 1.

Table 1. Shared situation awareness requirements. [11]

Level 1 situation awaress: perception	System Environment Other team members
Level 2 situation awareness: comprehension	Status relevant to own goals/requirements Status relevant to other's goals/requirements Impact of own actions on others Impact of other's actions on self and overall goal
Level 3 situation awareness: projection	Actions of team members

In addition to actor's own situation awareness requirements, actors have to fulfill the requirements set by the needs for shared situation awareness. The level 1 shared situation awareness requires the perception of other team members' information in order to fulfill the requirements. The level 2 shared situation awareness requires the comprehension of own and others' goals and requirements and understanding the impact of own actions on others and vice versa. To fulfill the level 3 shared situation awareness, the actor has to be able to project the future actions of team members. [11]

It is important to have a good team and shared situation awareness in order to perform actions correctly. For example in 1989 a Boeing 737-400 aircraft crashed in Kegworth, United Kingdom because the pilot turned off the wrong engine. The flight attendants and passengers were aware of the engine on fire but the information was never passed forward to the pilots. Before the crash the pilot broadcasted that there was an issue on the right engine when in fact it was on the left one. Passengers and flight attendants assumed that the pilot made a mistake while broadcasting and did not forward the information to the pilot, resulting in a crash. [12] In 2003 insufficient information exchange between the Italian and Swiss operators prevented the forming of high level situation awareness and resulted in a blackout of the entire Italian peninsula. [11] In 2006 the lack of good situation awareness of operators caused the central European grid to split into three islands with significant power imbalances in each area. [13]

It is also necessary to support the situation awareness of groups that consist of teams. This is often a case that the literature in the field does not discuss. For example in disturbances of electricity supply there are multiple actors which consist of multiple team members and each team member's situation awareness must be shared with others. Each actors' situation awareness composes a part of the whole group's situation awareness. [14]

3 Designing for situation awareness

Endsley [1] defines multiple general principles for designing user interfaces for situation awareness. Before applying the design principles, a situation awareness requirements analysis should be conducted. A situation awareness requirements analysis is an analysis that includes multiple different considerations. An operational concept is defined in order to describe the vision of how the system will be used. The concept includes the types of missions or functions that should be done using the system and also the system capability requirements from the operator.

Environmental conditions such as ambient noise levels are also taken into account in the design process. In addition to these user characteristics should be identified. These include characteristics like gender, skill levels and special clothing. [1]

Operational requirements of the operators should be determined. These include how the operators work, the types of processes they utilize and the operators' need for interaction with other actors. [1]

Endsley's [1] principles for designing for situation awareness can be divided into three logical groups. The first group includes principles that guide how information should be organized. The second group includes principles that guide how information should be processed. The third group includes other principles that help to improve the situation awareness of the operator.

3.1 Organizing information

Information should be organized around the operator's main goals instead of a technology-oriented way. Information should not be displayed based on the sensors or the systems generating the information. Information related to a particular goal should be co-located and should help to improve the decision making related to the goal. In order to determine the information required by each goal, a situation awareness requirements analysis should be conducted. The information gained from the analysis should guide the grouping of information across the user interface and ensure all needed information is provided. [1]

A common problem for situation awareness is tunnel vision. When an operator's attention is directed to a subset of information, the operator might miss critical cues about the current situation elsewhere in the operation area lowering the situation awareness of the operator. Designs that do not provide operator with a view of the global situation contribute to the attentional narrowing. Excessive use of menus and windows in the user interface also contributes to the attentional narrowing. A global situation awareness view should always be provided. A global view discourages the attentional narrowing. Current goal related detailed information should also be provided simultaneously. Global situation awareness view is crucial for determining the highest priority goals at any given point of time. It also enables the projection of future events. [1]

The user interface should also support trade-offs between the goal-driven and data-driven processing. Goal-driven processing is supported by designing the user interface around operator's goals. Data driven processing is supported by displaying the global situation. Displaying the global situation guides operator to focus attention to higher priority goals. Both processing methods are important from the situation awareness point of view and need to be utilized. By ensuring that both approaches complement each other it is possible to improve the situation awareness of the operator.

3.2 Processing information

Processing the information is important in order to improve the operator's performance. In many domains it is likely that without processing the information it is very difficult to perceive all the necessary information to form good situation awareness. Processing reduces the operator's workload. Endsley [1] lists some principles for information processing to achieve better situation awareness.

Level 2 situation awareness information should be presented directly if possible in order to support the comprehension of the situation. As human attention capability and working memory are limited, information that is processed and integrated into level 2 situation awareness requirements will improve the situation awareness of the operator by reducing the workload and things the operator has to remember and work on. For example displaying the difference between the target value and the current value helps operator's operation as no calculating needs to be done by the operator. If both values are displayed the operator has to do the calculating by him or herself and do more work in order to achieve the same level of situation awareness. [1] For example displaying which actions are currently available for the operator based on the state helps the operator. If the operator has to manually calculate if it is acceptable to open a certain switch/breaker, the actions take longer to initiate and it is more likely that the operator's actions cause issues in the power grid.

A system should also provide assistance for level 3 situation awareness projections. Projection of future state is a demanding task for an operator and requires a well-developed mental model. A system that provides projections of events and states improves the level 3 situation awareness of the operator. Inexperienced operators benefit from projections even more as their own ability to project future states and events is weaker. In addition a user interface that provides projections of future also supports the operator's own ability to create projections. While a system should provide level 3 situation awareness information, it is often difficult to create system-generated projections of the situation. For some information this is simple. For example a trend display that displays the changes of a parameter over time can be very helpful for operators' ability to project future changes in the parameter. In power grid this could be for example a load flow over time display where the operator can see how the load flow changes. [1]

Information overload is an issue in complex systems. There could be thousands of events in the user interface of a complex system without any processing which is why it is important to filter unnecessary information to improve the situation awareness of the user. If too much information is shown on the user interface, it is likely that the operator misses critical cues about the situation. Information filtering should still be used carefully as it can lower the situation awareness of the operator. Using a computer to decide what to show to the operator usually degrades the situation awareness of the operator and should not be used extensively. [1]

Filtering the information lowers the global situation awareness of the operator. Situation awareness is developed by observing system dynamics and trends over time. In cases where the system filters some of the information, the situation awareness could be lower as the operator cannot observe all of the system dynamics and trends. Filtering information might reduce the operator's capability of projecting the future. If a system tries to filter information based on the current situation, information that is critical for projecting the future might be filtered out. On the other hand it is often difficult to define what is needed for future projections, which is why it is often difficult to perform filtering correctly. Individual differences between operators might also cause issues in filtering. Some operators might benefit from a certain type of filtering while others' situation awareness can degrade. Generally displaying the information in a clear way while allowing the operator to decide what to look at and what to filter, is better than computer-driven strategies for providing only subsets of information. This way the operator's ability to maintain high level of system and predictive awareness will be improved. [1]

3.3 Other principles

Critical cues for activating mental models and schemata need to be determined and made salient in the user interface as mental models and schemata are hypothesized to key features in achieving higher levels of situation awareness. For example in power grid operation if a certain switch-disconnector tripping triggers a situation (e.g. a hospital without electricity), a notification should be sent to the operator. The problem is that the critical clues are often very subtle and require years of experience to attend to. Because of this it is often very difficult to explain and thus cannot be added to user interface. In cases where the cue is explainable and important, it should be added to the user interface. [1]

Taking an advantage of parallel processing capabilities should be done when designing a situation awareness system. A person can only process a limited amount of information through certain sense. Utilizing multiple ways of sensing allows the operator to process more information. For example people can only process a certain amount of visually received information. Utilizing auditory information allows them to process more information. Similarly operators can process information felt through skin simultaneously with auditory and visual information. Even if an operator is very focused on a certain subset of information on a visual display, it is easy for the operator to react to a loud noise or a tactile feedback. [1]

4 Designing a situation awareness system for disturbances of electricity supply

In disturbances of electricity supply it is common to have multiple actors trying to recover from the outage. The actors have separate goals but they have to work together in order to recover as fast as possible. Due to this there is a need for a system to share the information of actors in order to improve the situation awareness of each actor. [14]

Distribution network company (DSO) is the main actor working on the restoration process. DSO's goal is to restore electricity to all consumers as fast as possible. During the restoration process the DSO has to prioritize restoration areas in order to minimize the losses caused by the outage. Usually this is done by prioritizing large important consumers like factories and hospitals. The issue is that small consumers can be critically electricity-dependent as well. In cases where a consumer has a ventilator, it is critical that the consumer is evacuated before the battery capacity of the ventilator runs out. It is difficult for DSOs to be aware of all critically electricity-dependent consumers. Maintaining a database of critically electricity-dependent customers requires a lot of resources. By having a maintained database the DSOs can target restoration actions based on the criticality of the site and not just the consumption of the site. [14]

Municipalities and special health care are responsible for many of the critically electricity-dependent people. It is crucial for them to know if any of the patients are without electricity supply. Without the knowledge authorities cannot perform necessary actions to ensure the safety of the patients. While the authorities are aware of the locations of the critically electricity-dependent people, it is difficult to combine the outage information with the location information.[14]

Another issue during the disturbances of electricity supply is the amount of systems actors have to use in order to maintain a high level of situation awareness. Users like municipalities and rescue services often have multiple distribution network operators in the area. The users have to switch between multiple systems just to get the necessary information of the electricity network situation. In addition the users need to use other systems like their own customer databases to get all the necessary information to form high level of situation awareness. This increases the workload of actors by a large amount making the operation more prone for errors. [8]

The situation awareness system attempts to fix the issues in sharing information between actors during power outages. The system combines information from multiple sources and displays the combined and refined information in a single display, reducing the workload of actors. A database for critically electricity-dependent consumers is maintained in the system by the users of the system, which saves the resources of the actors as they do not have to maintain own databases. The basic idea of the system is shown in figure 2.

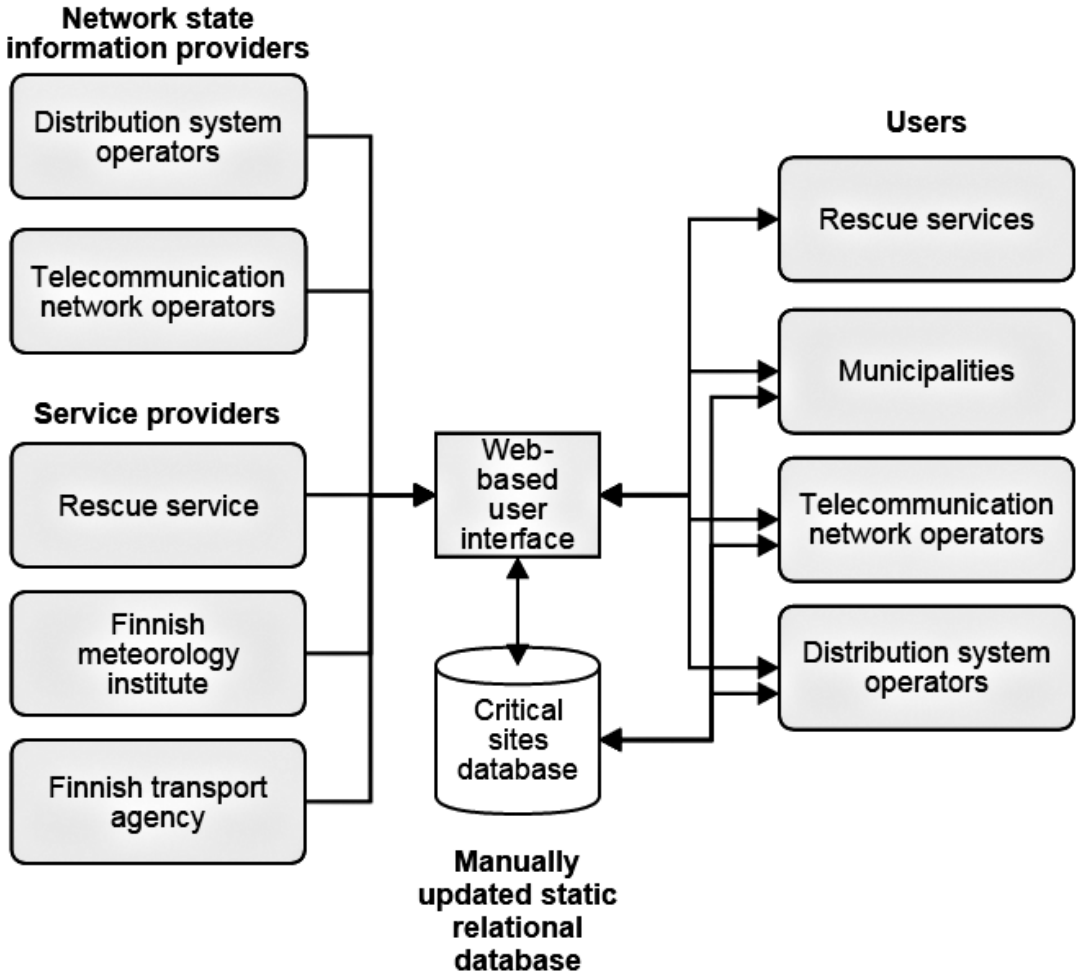


Figure 2. Diagram of the situation awareness system for disturbances of electricity supply

Network state information providers are data providers that provide real time data about the electricity and telecommunication networks such as status of each transformer in the network and the coverage areas of the mobile networks. Users provide critical site data that is combined by the system with the real time data in order to show the users of the system the current situation and which critically electricity-dependent or telecommunications-dependent sites are without electricity or telecommunications. In addition to real time network data and critical sites data the system retrieves information from auxiliary data providers such as the rescue services, Finnish meteorology institute and Finnish transport agency. These data providers provide data that is useful for planning actions.

The amount of information shared between users and data providers is huge and causes issues in the user interface design. It is crucial that users receive the information they need but it is also important that the user interface will not be cluttered with too much information.

The user interface of the system has been designed utilizing the design principles described by Endsley in [1]. The design principles have been applied to the design and the users have been interviewed about the user interface. The basic user interface is shown in figure 3.

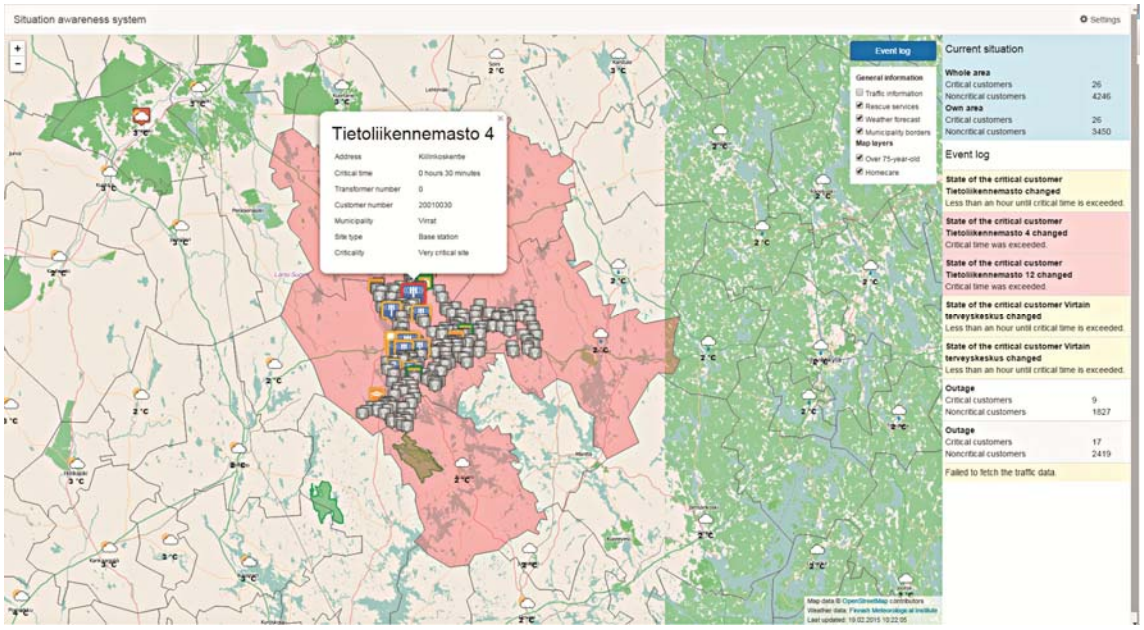


Figure 3. The main user interface of the situation awareness system for disturbances of electricity supply.

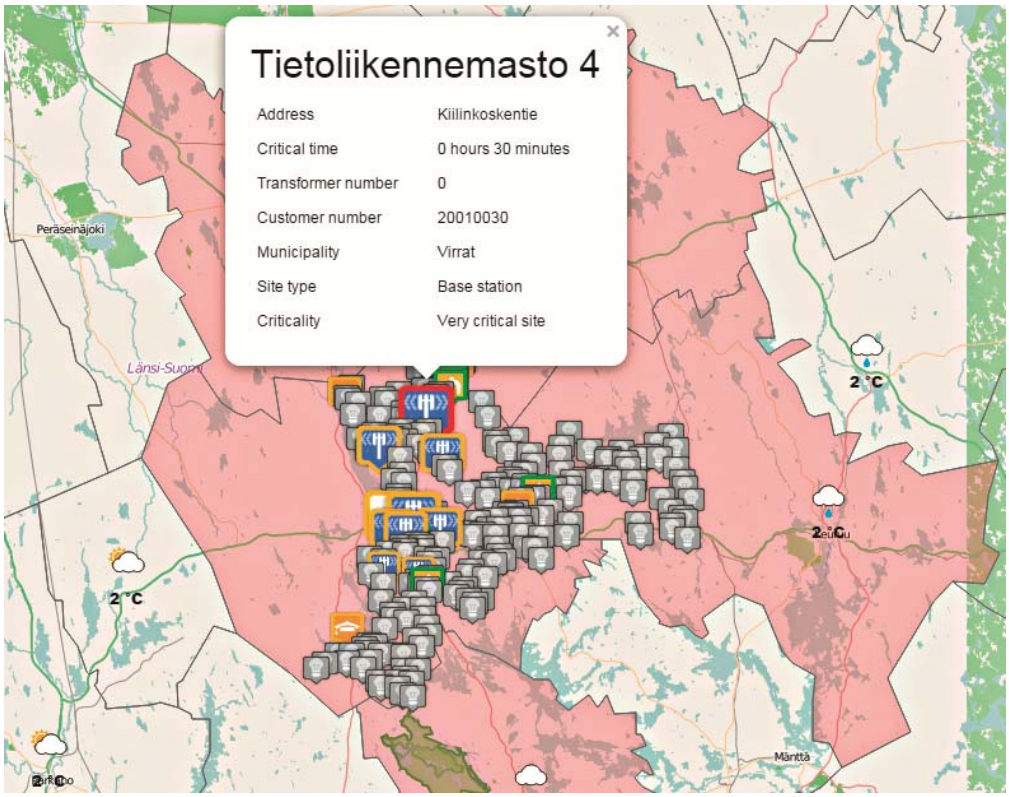


Figure 4. The map view.

The user interface is divided into two parts. The map view and the event log.

4.1 The map view

The map view is the main part of the user interface. By utilizing the map the user can easily see where the customers without electricity supply currently are. A range of information about customers without electricity is shown on the map. In addition additional information needed to restore the power to consumers is shown on the map. The map view can be seen in figure 4.

Transformers without electricity supply are shown on the map as grey markers. By showing the transformers without electricity supply it is possible to show areas without electricity. There are a lot of transformers in urban areas which makes it possible to identify users without electricity just by using the information about transformers without electricity supply.

In addition to transformers critical sites are displayed on the map. Each critical site type has own symbol. Critical sites are divided into three criticality levels:

Low criticality
Critical site
High criticality

The size of the symbol is defined by the criticality of the site. The size of the symbol increases as the criticality of the site increases. This way the most critical sites can be seen more easily. This directly supports the operators' ability to spot the critical cues (in this case the most critical sites) from the user interface. While the higher criticality sites are bigger they are still relatively small in order to prevent them from blocking other necessary information.

Critical sites also have a real time state. The state of the site is expressed with the color of the symbol's outline. The state is based on the critical time of the site. Critical time is a time that the customer can be without electricity without causing major problems. For example a ventilator patient needs electricity for the ventilator. Ventilators have a backup battery which lasts for some hours. This is the critical time of a ventilator patient as when the critical time exceeds, the ventilator patient will have issues breathing. Critical site states are divided into three states:

More than an hour until critical time will exceed. (green)
Less than an hour until critical time will exceed. (yellow)
Critical time has exceeded. (red)

The state of the site can be seen from the outline of the symbol. When the outline is green, it takes more than one hour until the critical time will exceed. When the outline is yellow, it takes less than one hour until critical time will exceed. When the outline is red, critical time has exceeded. This way of displaying the states supports the principle defined by [1] that says that a system should support the forming both level 2 and 3 situation awareness. In this case instead of displaying how long the outage has lasted and how long the critical time is, a state is displayed that informs

the user how long it takes until critical time will exceed. By displaying just the duration and the critical time the operator has to calculate the difference, which increases the workload of the operator. In the case of multiple critical sites being on top of each other when zoomed out in the map view, the view renders the most critical site on top of the others.

The colors of the outlines were selected in order to make the most critical cues the easiest to spot on the user interface. The red outline of the symbol can be spotted easily even if there are thousands of other markers on the view at the moment, granted the other symbols do not have red outlines as well.

By clicking a critical site the user can see more detailed information about each site. When user clicks a site, a popup window will open which shows information about site's criticality, state, address information and other useful information. This way the operator does not have to fetch the information from a customer information system or similar system. Hiding this information behind a popup clarifies the view. This also does not hide the information needed to form good situation awareness, though. Operators are usually not interested in the sites that have no outage but instead the ones without electricity.

Critical sites can be split to different map layers. This eases the displaying of information in situations where there are a lot of sites. For example municipalities want to see all over 75-year-old tenants. There are a lot of over 75-year-old tenants which can cause issues if they are shown on the map permanently. Map layers can be hidden from the map which clarifies the view. According to [1] filtering should be done carefully and control should be given to operator instead of system deciding what to filter. This has been taken into account in the design. Operators can decide what they want to filter and can also look at the global situation if needed. In this case it is important to allow filtering as other actors such as DSOs are not interested in seeing all over 75-year-old tenants.

In addition to transformers and critical sites other information is shown on the map. To improve the situation awareness of actors a weather forecast, current traffic situation in the area, rescue services activity and municipality borders are displayed on the map. Normally actors have multiple sources of information that is used to form the situation awareness. This increases the workload of the operator as they have to focus on multiple displays or switch between multiple windows in order to gather all necessary information. By displaying all information in a single view the user has a lower workload.

Some of the other information can be used to project future events. For example weather forecasts help actors to plan actions based on the weather. If the temperature increases a lot during a cold winter day a few hours after a power outage started, it is likely that people do not have to be evacuated. On the other hand if the temperature drops even lower, it is likely that the apartments will get colder faster and evacuations are needed.

Municipality borders are shown in the map view in order to show which municipalities are affected by the outage. Operators can also see how many critical and normal customers are without electricity. Operators can also filter the information to just own area information.

4.2 The event log

The event log is on the right side of the map view. It contains information about current situation in own area and also in the whole country. The operators define their own area as a list of municipalities of interest. Operators receive information about critical and non-critical sites without electricity in own area which improves the global situation awareness.

The event log shows the changes in the electricity network state in chronological order. New outages and related information such as how many critical sites are affected are added to the event log. Whenever a new separate outage occurs in the network, it is added to the log.

In addition the event log lists critical site state changes. The state colors used in the symbol outlines apply in the event log as well. For example when the state of the site changes from green to yellow (less than an hour until critical time will exceed) a new entry with yellow background will be added. The entry contains the timestamp and the site that was affected by the state change. The state change in the map view might go unnoticed if there are a lot of critical sites without electricity on the map. The event log helps the user to notice the changes in the state as the user will notice the new entry and act based on them.

An example situation is shown in figure 5. In the figure the current situation in the country and own area can be seen on the top. The user can see, how many customers in the own area are currently affected and how many are in the whole country. This gives the user a good idea about the whole situation, not just the own area. This is important as different actors often have to support other areas' operations.

In the example the log lists changes of state for a health center and three telecommunications base stations. In the figure the timestamps of each log entry are missing and will be added in the future.

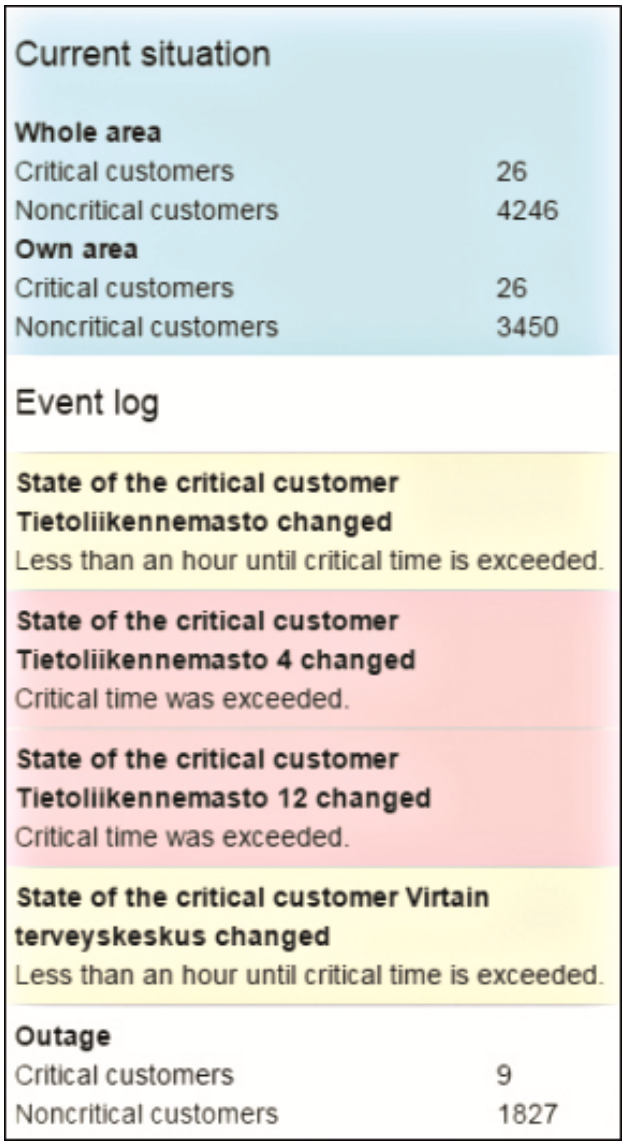


Figure 5. The event log.

4.3 Future development

The system is still under development and testing needs to be done. Some of the design principles defined in [1] have not been used yet. For example no parallel processing capabilities are currently utilized in the system. Due to multiple different actors using the system, it is highly unlikely that every actor can afford more advanced user interface (for example tactile). It also increases the difficulty of adopting the system in operation reducing the likelihood of actors adopting it. It is also likely that utilizing tactile sense is difficult in the domain. Auditory information has been discussed but auditory cues often distract the operator and should only be used for the most critical events. As the power outage progresses more slowly than for example a power plant operation fault, it is usually not crucial to perform actions in a matter of seconds. Most crucial actions like triggering a switch/breaker happen automatically in milliseconds. Auditory information should help the operator to notice critical issues but this is not usually necessary during the power outage restoration process.

A live demonstration with real live data from mobile and electricity networks is under development. During the live demonstration the actors that are active during disturbances of electricity supply will be able to test the system and the user interface during an actual power outage. The information received from the live demonstration should help in improving the system.

5 Conclusion

Endsley's model for situation awareness is a widely used model in different domains such as aviation and military operations. The model defines three levels of situation awareness that simplifies the measurement of situation awareness of operators during operation. This allows the system designers to more easily design user interfaces for improving the situation awareness of operators.

Endsley's design principles can be divided into three logical parts. How to organize information, how to process information and other principles for designing user interfaces for situation awareness. These design principles can be used to design user interfaces that are capable of providing high level of situation awareness to operators.

Designing user interfaces for situation awareness for disturbance management in disturbances of electricity supply is challenging. In the domain there are multiple different actors with varying goals. All actors main goal is to return to the normal state and minimize damages but achieving this goal is done in different ways. Actors' goals are loosely linked. Actors need to exchange data and this data has to be displayed in a clear manner. The situation awareness system for disturbance management, designed using Endsley's principles, tries to address the issues found in research and in practise in order to improve the recovery process and reduce the costs of disturbances of electricity supply.

References

[1] Endsley, M. & Jones, D., *Designing for Situation Awareness*, CRC Press, 2011

[2] Endsley, M., *Toward a theory of situation awareness in dynamic systems*, Human Factors, vol. 37, 1995

[3] Smith, K. & Hancock, P.A., *Situation awareness is adaptive, externally directed consciousness*, The Journal of the Human Factors and Ergonomics Society, March 1995

[4] Bedny, G. & Meister, D., *Theory of Activity and Situation Awareness*, International Journal of Cognitive Ergonomics, vol. 3, No. 1, 1999

[5] Sorensen, L., Stanton, N., Banks, A., *Back to SA school: contrasting three approaches to situation awareness in the cockpit*. Theoretical Issues in Ergonomics Science, 2011

[6] Endsley, M., *Situation awareness Misconceptions and Misunderstandings,* Journal of Cognitive Engineering and Decision Making, Vol. 9, No. 1, March 2015.

[7] Panteli, M., Crossley, P., Kirschen, D., Sobajic, D., *Assessing the Impact of Insufficient Situation Awareness on Power System Operation*, IEEE Transactions on Power Systems, Vol. 28, No. 3, August 2013.

[8] Haapanen, J. *Tilannekuvan hyödyntäminen sähkö- ja tietoliikenneverkkojen häiriöissä (Utilization of situation awareness in disturbances of electricity and telecommunication networks,* in Finnish*),* Master of Science Thesis, Tampere University of Technology, Tampere, 2015

[9] Jones, D. & Endsley, M., *Sources of situation awareness errors in complex environments*, Human Factors, vol. 42, 1996

[10] Manninen, J. *Visualization requirements and concepts for a combined SCADA and distribution management system*, Master of Science thesis, Tampere University of Technology, Tampere, 2014

[11] Panteli, M. & Kirschen, D. *Situation awareness in power systems: Theory, challenges and applications,* Elsevier, Electric Power Systems Research 122, 2015.

[12] *Report on the accident to Boeing 737-400 G-OBME near Kegworth, Leicestershire on 8 January 1989*. https://assets.digital.cabinet-office.gov.uk/media/ 5422fefeed 915d13710009ed/4-1990_G-OBME.pdf cited 11.8.2015

[13] Union for the co-ordination of transmission of electricity, *Final Report, System Disturbance on 4 November 2006,* 2007

[14] Krohns-Välimäki, H., Haapanen, J., Aalto, H., Strandén, J., and Verho, P., *Demonstration of the inter-organizational situation awareness system to major disturbances*, 23rd International Conference on Electricity Distribution, 2015

Situation Awareness in Distributed Teams and Some Methods to Improve It

Niina Nissinen
Finnish National Defence University
niina.nissinen@mil.fi

Abstract

The aim of this study is to examine situation awareness and methods to improve its quality in distributed team operations. The research paper is based on literature study, emphasizing especially the book *Designing for the Situation Awareness* by Mica R. Endsley. First the theory of situation awareness is explained shortly. Then a few methods to improve team situation awareness in distributed teams are introduced. Finally the results are discussed. This study is a part of a postgraduate seminar, which was organized by the Department of Military Technology in 2015.

Keywords

Situation awareness, Team operations, Distributed teams

1 Introduction

Correct information is crucial when trying to maintain situation awareness. Any information that spreads among the troops has an influence in their individual and team situation awareness's and the quality of situation awareness effects directly to decision-making. The decisions that are based on false information can have serious or even fatal consequences in a battlefield. During operations, however, up-to-date information might be hard to get, especially when troops are decentralized along a battle space.

Distributed teams are present in every military domain. In air operations pilots usually work physically alone in their cockpits. They get situation data by observing environment and different meters visually, and by communicating with others via radios. In sea domain navy vessels constitute a system where each ship or boat is a unit with a specific crew. Situation data is gathered by observing meters and environment, and by communicating with others directly or via different devices. In land operations troops are organised in units and then distributed to a battlefield where they communicate mainly via radios.

To tackle the fog of war -the uncertainty in situation awareness during military operations- high level of team situation awareness is needed. Successful operations require that actions and different phases of the operation have been synchronized rigorously, which in turn demand seamless co-operation between military branches, different units and individual soldiers. All actors who are involved in an operation

have to be aware of a current situation, tasks and locations of friendly and hostile forces. It is essential especially in dynamic and fast situations as in air operations.

Experiences from the World War II emphasized surprise when trying to achieve victories in air combats. For example German pilot Erich Hartmann with 352 victories from WWII noted that before opening fire, 80% of devastated enemies never knew that he was there. The phenomenon was noticed also during the Vietnamese war when analytics showed that 81% of friendly and enemy defeats were caused because pilots either never noticed a threat or noticed it so late that there was no time to react. The state in which a pilot was shot down due to successful surprise was called the breakdown of situation awareness. [10]

Usually complex and dynamic systems are full of elements that can disturb concentration on certain tasks. An excessive data flow and excess information can lead to breakdowns of situation awareness and cause several problems when individual's data processing capacity is exceeded. Also, when team members are located in different places they might have problems in developing situation awareness of on-going tasks. That, in turn, might cause flaws in the progression of the whole operation.

The purpose of this study is to examine situation awareness in distributed teams and to survey the most important factors affecting it. The concept of situation awareness for individuals and for teams is introduced in chapter 2. Critical factors and processes that affect in situation awareness are described in the same chapter. Chapter 3 concentrates on some general design principles that can help to enhance individual and shared situation awareness, and further performance of the whole team. Chapter 4 concludes a few main points of the topic and in chapter 5 there is a short discussion of the concept of situation awareness. This study is based on the book "*Designing for Situation Awareness"* by Mica R. Endsley and is a part of the postgraduate seminar, which was organized by the Department of Military Technology in 2015.

2 On Situation Awareness

2.1 The Concept of Situation Awareness

Situation awareness (SA) is a specific knowledge that is needed for an effective decision-making, especially in the case of dynamic and fast situations. The situation awareness research is originated from the military aviation domain where good SA is critical but hard to achieve [3]. In the aviation context SA is defined as an ability to develop and sustain consciousness in air combat situations of where participants are located, what they are currently doing, and where they might be in the immediate future [10].

A more common definition for the situation awareness is

"the perception of the elements in the environment within a volume of time and space, comprehension of their meaning, and the projection of their status in the near future" [1].

According to the definition, situation awareness is thus a composition of three cognitive processes that are perception, comprehension, and projection. Achieving situation awareness then depends on the ability to perceive relevant signals from an operational environment, to process the observed data to form a specific comprehension of the situation and to project its possible impacts on the current situation [2]. The model of SA in dynamic decision-making situations is presented in figure 1. All three levels of situation awareness – perception, comprehension and projection are presented in the core of the model.

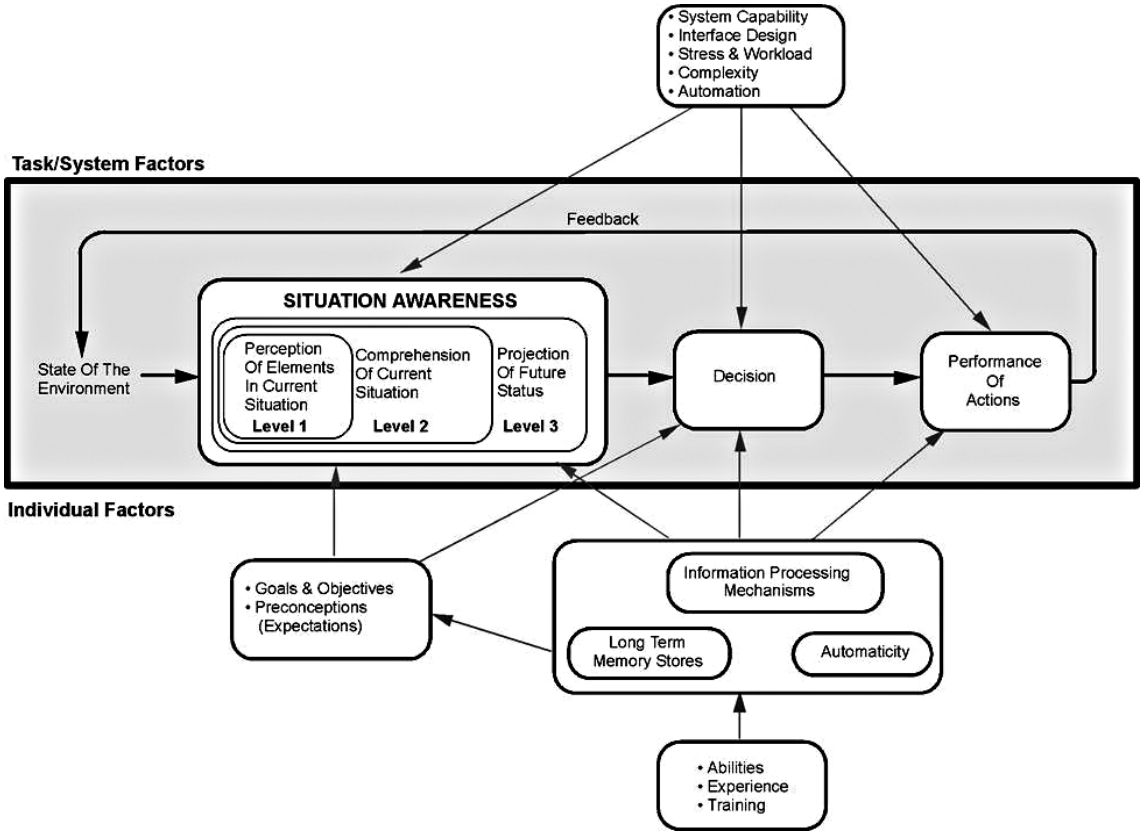


Figure 1. Situation awareness model in dynamic decision-making [3].

Good situation awareness means that an actor is aware what is currently going on, what consequences present situation might have in the near future and what kind of actions are required in that certain situation to operate successfully. Situation Awareness is a product of personal experiences and individual knowledge. The quality of SA is influenced by the limitations of a human's cognitive capacity. For example, a short-term memory can sustain about seven blocks of information simultaneously [6]. If this capacity is exceeded, relevant information might be lost and it could lead to incorrect conclusions [4] and wrong decisions.

2.2 Shared Situation Awareness

The ability to share personal situation awareness is essential especially when working as a team. A team is a group of people who work together to achieve a common goal or an objective [8]. Key factors that are needed for a successful operation are a common goal for the whole team, a specific role for each team member, and individual tasks that overlap [11]. A common goal motivates and gives purpose for a team effort by specifying what team members have to achieve as a group while specific roles define individual goals for each [1].

The roles and individual goals should be interdependent and overlap so that personal SAs could be shared and the team would be able to form a common situation awareness (see figure 2). Correct and shared situation awareness is essential for efficient teamwork. The definition for shared situation awareness (SSA) is

"the degree to which team members have the same SA on shared SA requirements" [3].

Basically shared situation awareness means that every team member understands the present situation similarly. When there is a common understanding of the situation and shared situation awareness exists the actions can be synchronized more easily [7]. The way human brain process information depends on people's individual and unique backgrounds such as education, experiences or hobbies. Hence the situation awareness is not identical between any two humans, even if they had the same data available. Whether the team has the same data in the same circumstances the SA can vary widely within a team. [3]

Since team members have different tasks they don't even need identical situation awareness. It only has to be adequate. Team members have their own specific tasks, and the data needed to accomplish them varies. What is required is the knowledge of elements that are common for different tasks. The overlapping elements then define the data whose status should be shared with others. Especially when the team is distributed by time (e.g. time zones or rotating shifts), distance (e.g. geographical location or workspaces), or other obstacles. [3] For example military operations have always been divided in multiple phases along timeline and multiple units that are separated geographically. Operations were coordinated then by centralized plans, guiding what unit is doing which task and when.

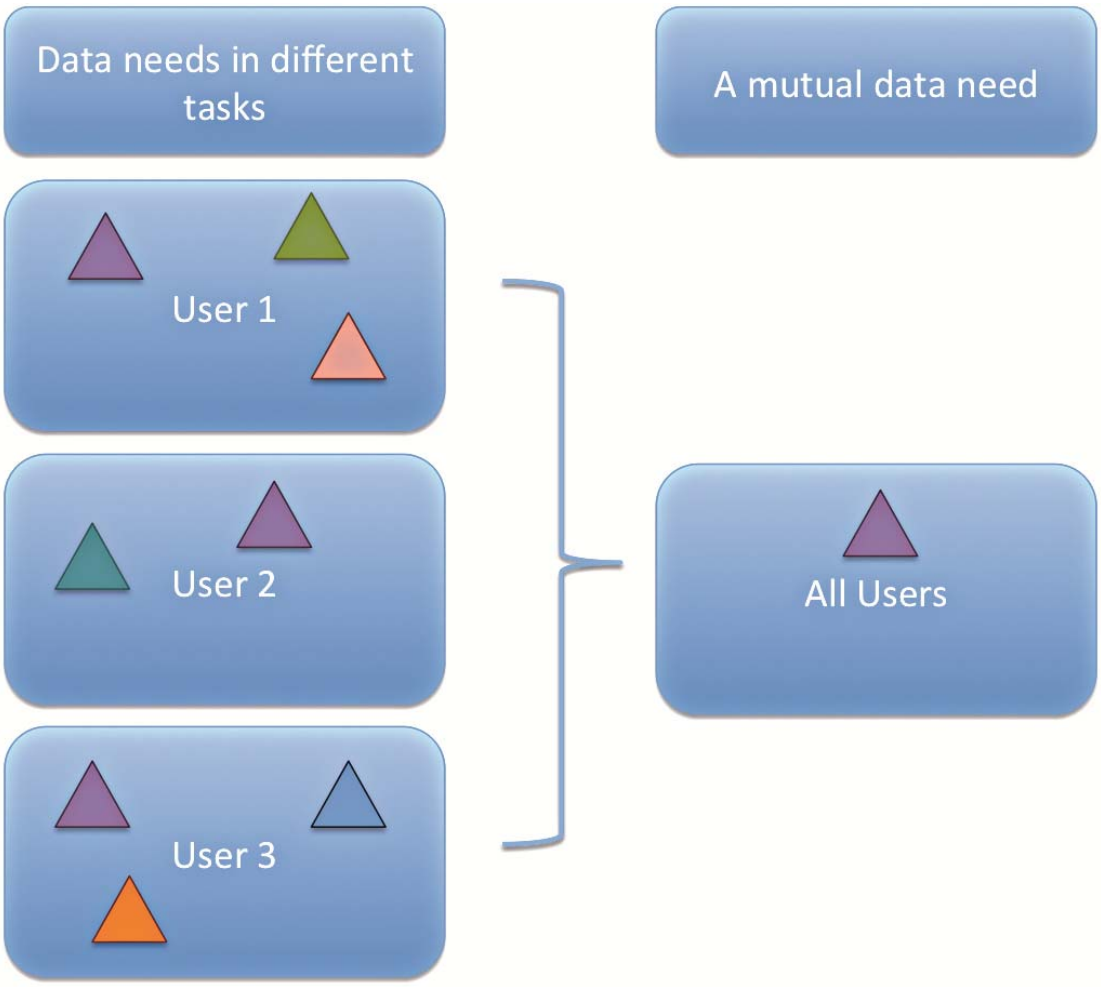


Figure 2. Shared situation awareness – an overlap in data needs

2.3 Critical Factors Affecting Shared Situation Awareness

Team situation awareness model includes four critical and interdependent elements that affect the development of team SA and the sharing of situation awareness within a team. The elements are devices, mechanisms, processes, and requirements. All of them are needed to form a successful team SA. Critical factors and their relations are presented in figure 3 [3].

2.3.1 SA Requirements

The SA requirements analysis defines all the elements that have to be shared between team members at all levels of SA (perception, comprehension, projection) to achieve correct shared situation awareness. It is not necessary to share every detail to everyone in a team. Overlaps in team's information needs are the elements that improve common understanding of the situation and should be shared for all. Knowledge of a common goal, individual tasks and their current phases is therefore important. [3].

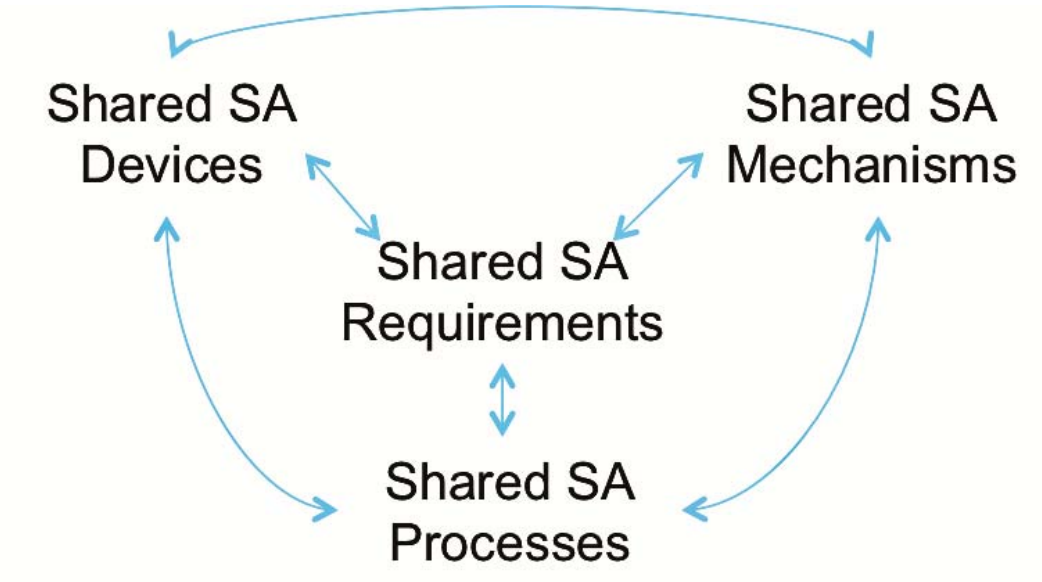


Figure 3. Four major factors for the development of good team SA and shared SA in teams [3].

2.3.2 SA Devices

Shared situation awareness can be supported by multiple devices, which transmit visual or audio data. SA devices that are used when creating team SA are means of communication, shared environment, and shared displays.

Verbal communication is often considered as the most significant part of communication but people communicate also non-verbally. Body language like facial expressions or expressive behaviour can be even more important than words. Whether verbal or non-verbal, the communication should be efficient. The most effective way to improve communication and team SA is to operate physically in the same place with other team members. Communication is spontaneous when there is no need to use external devices to contact others. Non-verbal signals are easier to observe and interpret when the whole team is staying at the same place. In addition the physical changes in a situation or an operational environment (e.g. temperature) can be felt when working at the common space. [3]

Displays that are in common use improve creating shared situation awareness. If team members need some specific information from others, they can just check it from the common displays. The ability to get relevant data quickly is essential especially when situation is changing fast or crucial decisions concerning present tasks should be made. Transmitting relevant information on displays remains, however, a central challenge. The choice of data that needs to be screened and the amount of details that should be shown are always case sensitive. Also the visualization of data is problematic especially when team members are from several organizations or represent different authorities. Despite of the benefits of shared displays, the research has shown that they reduce direct communication. Then people concentrate only on the information that is presented on displays. [3]

2.3.3 SA Mechanisms

In addition to devices and communication skills, there are certain internal mechanisms that have an influence when sharing individual SAs with other team members. Probably the most significant of those mechanisms is a mental model. That model is a psychological representation of an environment and its assumed behaviour. Situation awareness is an abstract and dynamic phenomenon and mental models serve as frameworks to explain current situation and to estimate the future states of a system [7]. A chart in figure 4 presents relations between mental model and SA.

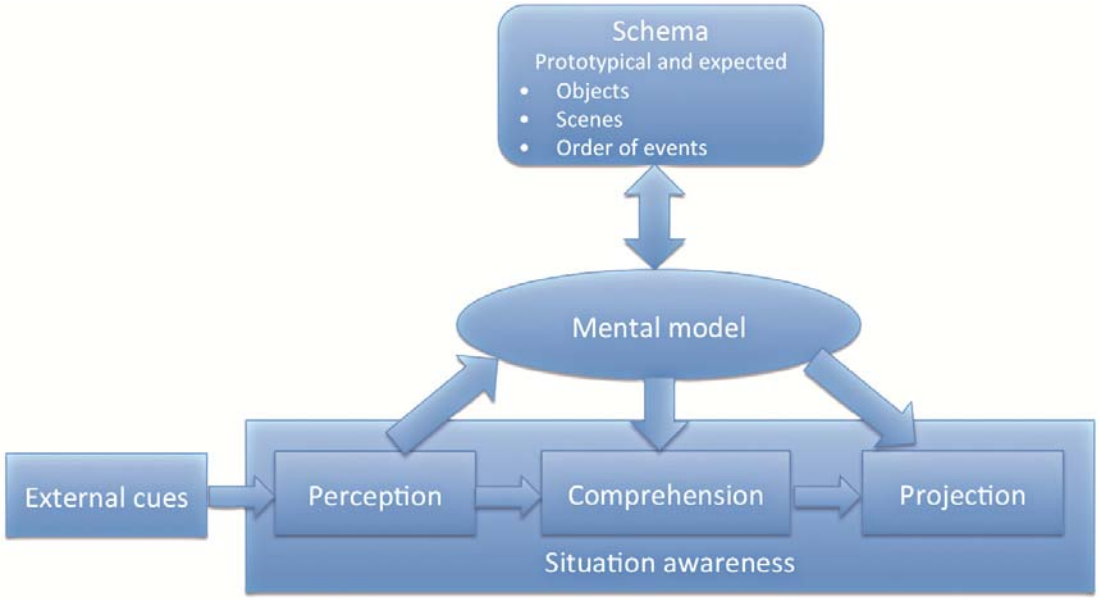


Figure 4. Schema, mental model, and situation awareness according to Endsley [3].

Training and common exercises support the development of a common mental model. Mutual experiences form a common ground for collaboration. A common ground is a frame of reference [5] and it means elements that are somehow mutual for all team members. A common ground can be for example a set of specific concepts or symbols that are familiar for all. Education, studies, courses or even cultural background are seeds for a common ground.

Common mental models have several advantages. They help to build shared situation awareness for a team. They also help to focus actions toward a common goal. Teamwork is more effective when other team members and their tasks are familiar. Therefore the team should train together and gather experience on each other's tasks and positions. Cross-trained teams have been shown to be more productive than the teams whose members have no experience on each other's tasks [3]. When a team uses common concepts, communicates effectively, and knows tasks in other positions, the team behaviour is predictable in some degree, which in turn enhances the collaboration and response in acute situations.

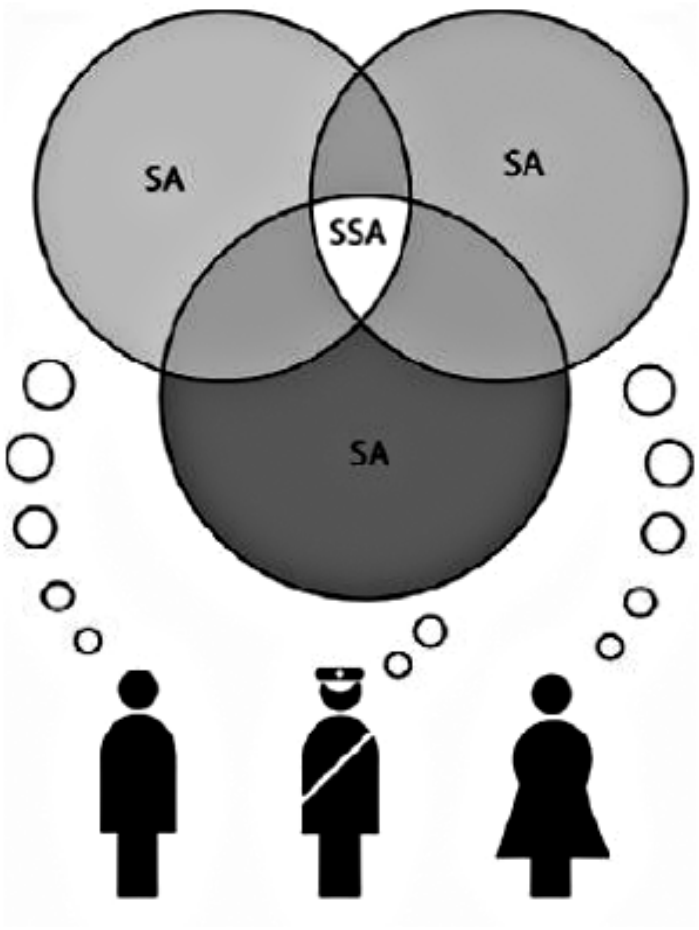


Figure 5. Common Ground (Virrantaus & Mäkelä, 2008)

2.3.4 SA Processes

The development of shared situation awareness is dependent on good processes, which make teams work more productive. Effective teams have plans for contingency, which improve the projections of what might happen in the near future. Effective teams have leaders who set a common goal as well as personal goals. The leaders promote information sharing and communicate strategies, plans, and intentions to help team members to build their individual situation awareness on the same expectations and foundations. They rationalize their decisions and provide estimates, predictions and warnings of possible future actions. [3].

Effective teams put an effort to gain a shared understanding of tasks and common goals, which is necessary especially when a team consists of people with different backgrounds. Effective teams encourage other team members to express their possible variant opinions and visions. According to research, ineffective teams commit to three major mistakes that are misunderstanding the information, approval of poor situation awareness, and the poor organizational culture and processes. Ineffective teams may lack common objectives or the objectives are very indefinite. They may not have personal tasks at all or their tasks do not serve the common goal. Ineffective teams have often poor leaders. [3].

2.4 Breakdowns in Situation Awareness

A Breakdown in situation awareness means that a person does not know what is currently happening in the operational environment. [10] When working in distributed teams, the risk for breakdowns in SA is great. Breakdowns can occur for multiple reasons. Team members can understand the signals from environment and the elements of present situation differently. Task-specific concepts can be misunderstood or they can have different meanings for different members. [3]. For example in different military branches (army, navy, air force) certain concepts can be understood in various ways. Or if team members are not for example native in English, some words might cause confusion. Divergent assumptions can cause interruptions to team SA too. A team member might assume that certain information is already shared to others while it is not. Breakdowns in team SA can happen if members can't interpret signals from environment correctly or the signals are just discarded. Multiple data sources can cause breakdowns in situation awareness as well. [3]. Figure 6 presents a principle of breakdown in situation awareness. The grey planes are aware of each other but do not see the green plane.

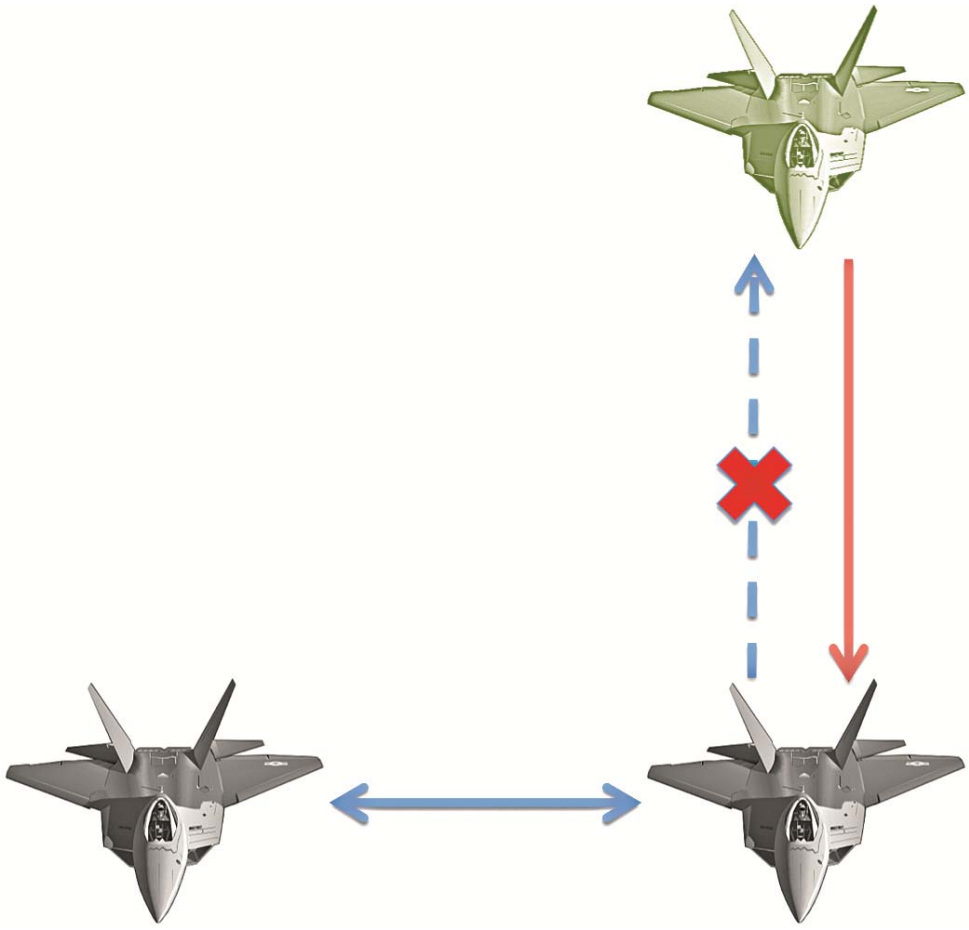


Figure 6. Breakdown of Situation Awareness.

3 Design Principles for Supporting Team Situation Awareness and Team Operations

Team situation awareness is a composition of individual mental models that have been shared between other team members. The ability to share an individual SA and mental model is crucial when building a team SA. Forming shared situation awareness and maintaining team SA is a challenging task. There are six design principles to improve team SA and further team operations.

3.1 Common operational picture COP

Probably the most well known resource when building, maintaining and updating situation awareness is a common operating picture (COP). The COP supports decision-making. It is a document that is built upon the situation data. The COP can be transmitted via technical devices and shared with other actors. It is used for the assessment of a situation, its cause and its effects as well as for the management of available resources [9].

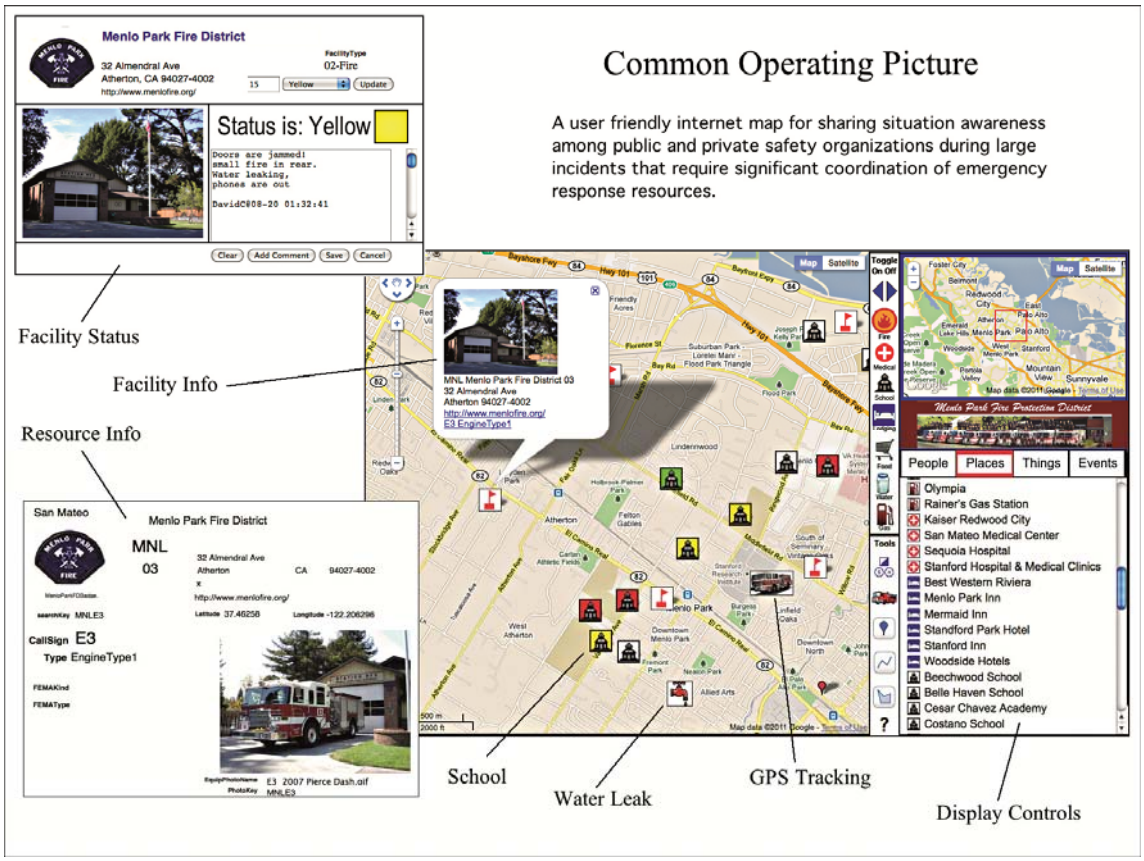


Figure 7. An example of a COP. [13]

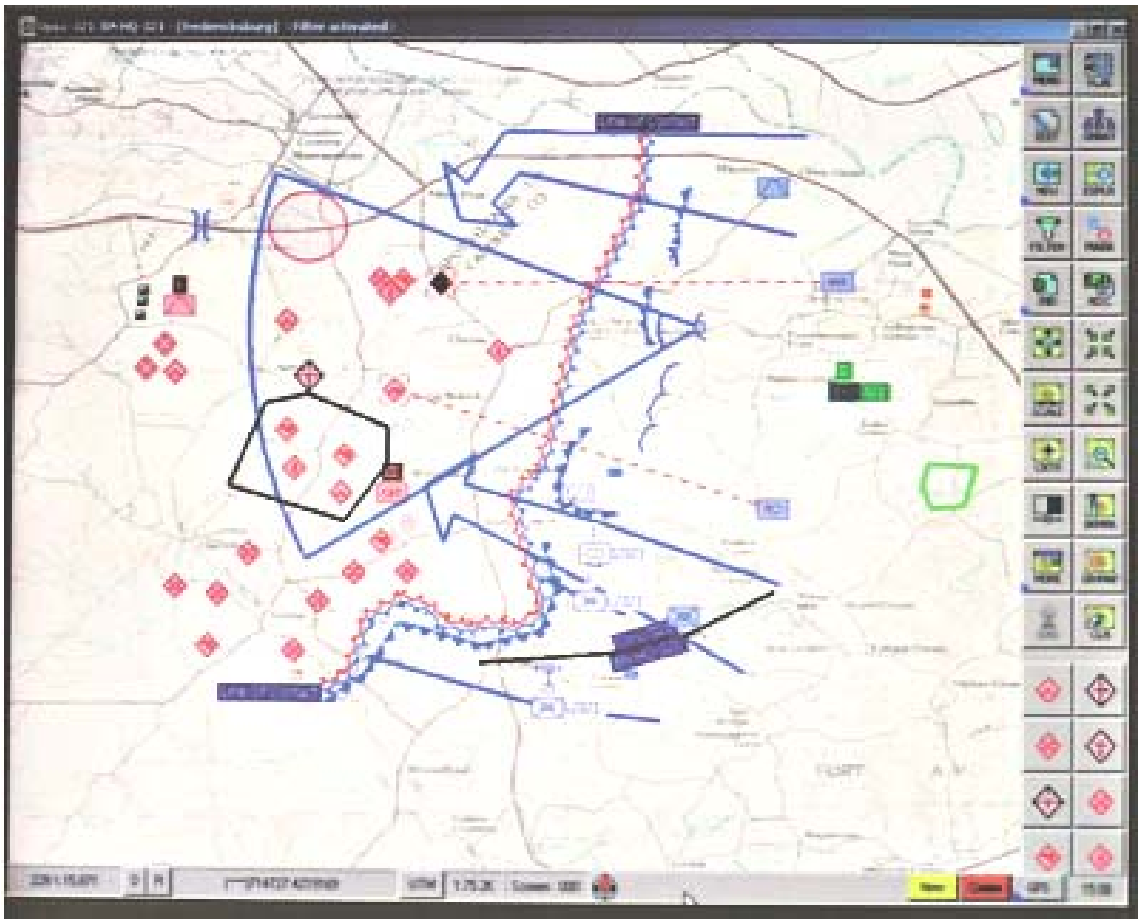


Figure 8. An example of a COP. [14]

The COP's content has to be relevant and it should be updated continuously. The data quality is essential. It has to be filtered and chosen carefully. If there are multiple data sources for similar information, the integration of data is crucial. Excessive information can cause SA breakdowns. Hence the overlaps in team members' information needs define what data should be chosen for the COP. The visualization of data has to be unambiguous, explicit and understandable for all team members. [3].

The good common operational picture mitigates sharing the situation awareness and further building the team SA [7]. When choosing the elements for a COP, it is crucial to consider the users and their needs: who is going to use the COP and for what purposes. The organizational cultures of different actors as well as the level of command define the extent and the amount of details that are needed for current situation. [3]. Examples of common operating pictures are presented in figures 7 and 8. Figure 7 presents an Internet based COP that is constructed for co-operation purposes. Figure 8 is an example of COP that could be used in a military context.

3.2 Flexibility of COP

The Common operational picture should be flexible so that only the data based on individual user's requirements are displayed. Even if the data is from the same database. Each team member can be located in a different geographical place and they all can have individual goal orientations. Therefore the data that is presented on COP should support user's objectives. In addition, team members with divergent backgrounds can have problems with terminology or symbols that are used on the COP. Hence flexibility is required at all levels of situation awareness when deciding which data should be displayed for different users. The level of operation and the branch have an influence on the data content of the COP. Also operational environment and time have an effect on the data selection. [3].

3.3 The Number of Displays

The number of displays in a team should be restricted. A single user is not able to focus on several displays simultaneously. Important data can be missed because relevant signals are hard to recognize among the data flow. Research has shown that a short-term memory can maintain only about seven blocks of information simultaneously [9]. To enhance the team situation awareness, each member should have an individual display that transmits the data only for that particular user. Any irrelevant data is forbidden. Excess information is confusing and the whole process can be delayed if the user is not able to find crucial information in time. [3].

3.4 Shifting Between Displays

The displays should offer a possibility to shift to other team members' displays even if personal displays have been optimized individually. Personal goals in different tasks may be interdependent so there might be a need to know in what phases of operation others are. Shared display system should allow the possibility to view the physical situation from different angles (physical shift) and to view the information in relation to various goal states (comparative shift) with different data filters. The possibility to shift to others' displays can build and maintain situation awareness. [3].

3.5 Visualization of Displays

The ability to adjust visualization of displays should be restricted from individual users. In many operations several team members are likely to use the same display and they are probably used to certain symbols and color codes. If this visualization is freely adjustable the ability to build and maintain situation awareness can decay because other users may not recognize new symbols or colours. [3]. Two different graphs are presented in figure 9 –the Red Cross and the Red Crescent- that are both symbols for the humanitarian aid. In Islamic countries a crescent is equivalent for a cross, which is a common symbol for Christianity. If a user of the COP is not aware of this cultural difference it might cause confusion and even delay the operation.

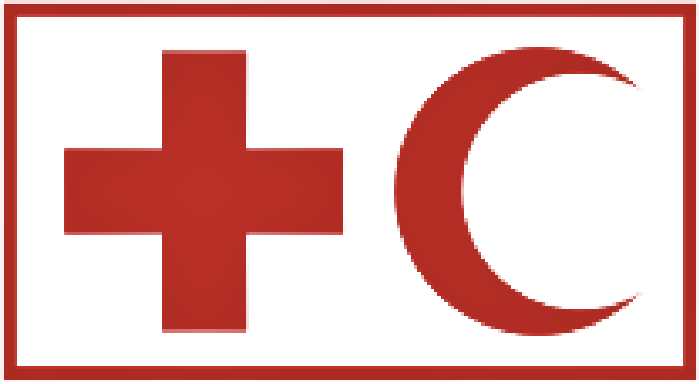


Figure 9. A visualization example [15].

3.6 Cross-Training

Shared situation awareness requires the knowledge of tasks and information needs of other team members. Hence the tasks should be cross-trained, which means that the team members practise in every position. Cross training helps communication. When the information needs are obvious to every team member the necessary data can be passed to others spontaneously. [3].

4 Conclusion

Situation awareness is a state of mind or condition where an actor observes signals from an operational environment, understands their meaning for the current situation and knows how to operate under those circumstances. In other words, the actor knows what is happening and what kind of actions are needed to handle the situation. In team operations each team member should be able to share their individual situation awareness between others and further constitute common situation awareness for the team.

The significance of team situation awareness is enhanced especially when there is a need for acute actions in current operation or the team is separated due to geography or time. The breakdowns in situation awareness can cause serious or even fatal accidents. Breakdowns can occur if a team is fresh or its members have different backgrounds, habits or concepts. Even excess data can cause breakdowns in individual and team SA. Team situation awareness can be improved by enhancing processes and procedures. There are certain technical devices available that can maintain achieved shared situation awareness.

5 Discussion

The most of the methods introduced in this paper emphasize the importance of different technical devices. The phenomenon itself is, however, a result of different psychological processes. To enhance the quality of individual and team situation awareness more attention should be paid towards human cognitive capabilities.

Maintaining high levels of situation awareness requires the ability to forecast how the situation changes due to different choices and actions that actors make. It is not enough to observe certain amount of elements from different devices but also to assess the relevance of data for current situation. If a team manages to achieve a high level of common situation awareness, it enhances the possibilities to be successful in their tasks although it does not permanently eliminate the possibility to fail. It doesn't matter how good a team's situation awareness was in the first place, the mission can still be unsuccessful for example due to lacks in decision-making or unfeasible tasks.

In a military context tasks and operations can fail because an opponent has better situation awareness. Situation awareness research is originated from military aviation domain, where high levels of situation awareness during the operations were critical and challenging to achieve. This was the case especially during the Second World War, where experiences emphasized surprise when pursuing a victory in air combat. Lately situation awareness research has spread to other branches as well. For example the new operating concept of the Finnish army emphasizes the importance of situation awareness during the operations.

Situation awareness as a phenomenon is not a new although the concept of SA might be. The phenomenon has existed as long as there has been life on Earth. Situation awareness is actually a result of all those cognitive processes that have been needed for surviving and for keeping people alive. Nowadays its significance is just somewhat changed and crucial is team operations between different authorities.

A high level of team situation awareness is challenging to achieve. Although there are certain processes and technical devices to enhance the quality of shared SA the technique is not crucial. Shared situation awareness is a result of effective communication between team members, whether it was verbal or non-verbal. Rehearsals, shared experiences and exact orders maintain the situation awareness regardless of random lapses in communication. But if the mutual exercises and training have not been possible, the communication is the only way to achieve objects.

"The key to success in war, certainly to success in combined operations, is lucid communication. Indeed, clarity of communication may be more valuable than combat skills" –General Paik Sun Yup

References

[1] Endsley, M., *Design and evaluation for situation awareness enhancement*. In proceedings of the human factors society 32nd annual meeting (pp. 97-101), Santa Monica, CA: Human Factors Society, 1998.

[2] Endsley, M., *Situation awareness analysis and measurement*. Lawrence Erlbaum, New Jersey, 2000.

[3] Endsley, M., *Designing for Situation Awareness. An approach to user-centered design*. 2nd Edition. CRC Press, Boca Raton, 2012.

[4] Guenther, R. K., *Human cognition*, Hamline University, Prentice Hall, College Div; 1 edition., 1997.

[5] Hunt, W.T., *Shared Understanding: Implications for Computer Supported Cooperative Work*, Department of Computer Science, University of Toronto, 1999.

[6] Miller, G. A., *The magical number seven plus or minus two: Some limits on our capacity for processing information*, Psychological Review, 63, pp. 81–97, 1956.

[7] Nofi, A., *Defining and measuring shared situation awareness*, Center for Naval Analyses, Virginia, 2000.

[8] Salas, E., Dickinson, T. L., Converse, S., and Tannenbaum, S. I., *Toward an understanding of team performance and training*, Norwood, New Jersey: Ablex, 1992.

[9] Seppänen, H. and Valtonen, V., *SAR prosessit (SAR processes)*, Volume 1, Number 2. Helsinki: National Defense University, Department of Tactics and Operations Art, 2008.

[10] Watts, B. D., *Clausewitzian friction and future war (revised edition)*, McNair paper 68, Institute for national strategic studies, National Defence University, Washington D.C., 2004.

[11] http://www.businessdictionary.com/definition/team.html cited 19.8.2015

[12] F-22 Raptor original figure from http://clipart-finder.com/clipart/f-22-raptor-bw.html cited 19.8.2015.

[13] http://www.cmu.edu/silicon-valley/dmi/files/images/cop-lg.jpg cited 19.8.2015

[14] http://dev.defense-update.com/wp-content/uploads/2012/01/TORC2H-DAP.jpg cited 19.8.2015

[15] https://fi.wikipedia.org/wiki/Punaisen_Ristin_ja_Punaisen_Puolikuun_yhdistysten_kansainv%C3%A4linen_liitto cited 19.8.2015.

Business Resilient Vulnerability Analysis for Dynamic High Security Environment

Klaus Zaerens
Finnish National Defence University
klaus.zaerens@iki.fi

Abstract

Vulnerability analysis methods have gained more interest in recent years, because of publicity on international cyber attacks to critical infrastructure, emerging hactivism and business reconnaissance. From this basis there has been a lot of discussion about the costs of risk management in software development. In this paper we discuss vulnerability analysis in a critical system context. Critical system means here the system in which operative outage endangers the continuity of the organization. As a solution to expenses of the improved information security we define the concept of business resilience which gives a general reference on the relevant improvements to a system. We present an approach to determine the criticality of identified threat to our business. We also propose a methodology to utilize the business resilience properties on dynamic environment such as high security network used by the military. The discussion and views presented in this paper can be adopted in any organization with doubts concerning the sensitive and classified contents of current ICT systems in cloud computing.

Keywords

Vulnerability analysis; Risk Management; Survivability; Attack tree; Military

1 Introduction

Survivability and software vulnerabilities have been one of the top discussions in military systems for over twenty years. Same time as the technology evolves, threats to systems become more diverse and hard to identify. This has inspired the researchers to achieve modelling the environments and to change the threats to more computable form. There are various definitions to what a threat is, but we approach the definition specifically from the survivability point of view. Barbacci introduced survivability as "System class, that is able to execute task in reasonable time, even if significant parts are paralyzed because of an attack or damage" [1]. According to that, we define the threat as an event that endangers survivability.

In this paper, we will discuss resource optimization when implementing vulnerability analysis in core authority systems. We define the key properties of such analysis. We also characterize the algorithms on how the analysis can be made on real-time basis in dynamic environment. We will narrow our observations to military systems in which the need for computational capacity is high and the reliability of information is always critical.

Economical risk management is optimization of resources in relation of identified threats and consequence damages. Systems cannot ever be built fully secured because of limited resources such as finances, expertise or time and ever evolving polymorphic environments. As a solution to modelling problem of such challenge in public authority environments, we propose a new concept called Business Resilience, which also improves information security in overall system.

We also propose a combination of a higher and lower level vulnerability analysis methodologies which enables us to address investment to a component where we can gain the most profit of the information security improvement. With higher level vulnerability analysis we can construct an overall understanding of the system and cover the issues with the infrastructure level security and the information security as a concept. After this we can focus to more detailed components on the system, for example individual software or the operation of the system. With this we can divide and address the budget to smaller fragments with the most financially effective way.

The paper proceeds as follows. First, we will examine the essence of vulnerability analysis by introducing relevant research of the field, defining its relevant terminology, characteristics and principles, as well as the benefits of the methodology within the scope of a military context. Next, we discuss on the business resilience concept and its key properties. Lastly, we propose algorithms to implement business resilience in a dynamic high security environment. We will conclude with key findings and a description of the future of business resilience in the military context.

2 About Vulnerability Analysis and Related Work

Vulnerability analysis is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. Modelling the critical infrastructure and identifying the most severe vulnerabilities are one of the key tasks for public officers in each country. The motivation for vulnerability analysis is also to have a measurable approach to policy making. It answers to the question that which components should be made more resilient to attacks and it determines the probability of a successful attack on a component. With combination of the component vulnerabilities and its probabilities on attack, one can quantitatively evaluate the vulnerability of a sector. However, the analysis is as comprehensive as the model accordingly.

There has been a lot of research on attack, vulnerability and risk analysis. Some of them are based on network specifications [2, 3, 4, 5], some exploits graph representations [2, 6, 7] and perhaps the most popular approach is utilizing tree constructions like attack tree or fault trees [2, 8, 9, 10]. Vulnerability analysis has a close relation to survivability analysis and research [11, 12, 13]. There is also more comprehensive approaches that combine several of the methodologies like model based vulnerability and risk analysis method for critical infrastructure of society like the one presented by Lewis [14]. It exploits the network modelling as well as fault tree analysis. Instead of analyzing the system environment of the components, we can approach the data contents by dynamic taint analysis (DTA) [15, 16, 17]. It is

very powerful method for detecting vulnerabilities in applications like the one Herrera presented for Java malware [17].

In this paper we adopt the approach presented by Lewis as a starting point [14], because of the scalability from the critical network infrastructure to the individual system component. With simplicity and practicality, it gives room for the additional methodologies and tools to enhance the presented risk assurance level. The main steps of model based vulnerability analysis and risk analysis are [14]:

Listing of assets. Identifying all the components of the system.

Network analysis. Categorizing and analyzing the relations of the components. Identifying the most critical component.

Fault tree analysis. Building a tree representation of the vulnerabilities to create a fault or failure in a component. With vulnerability probabilities, the likelihood of failure occurring in a component can be estimated.

Event tree analysis. The outputs of previous step are inputs into an event tree. An event tree contains all possible events obtained by single and multiple combinations of faults. With this step, assurance of all relevant vulnerabilities is enhanced.

Event matrix analysis. The processed number of events can be reduced with event matrix by enumerating the single and double faults from the event tree.

Risk Assessment and Resource Allocation. Determination of optimal allocation for funding to improve the components against the vulnerabilities.

In Lewis approach the components are determined and to each component possible faults and threats are identified. The components are to be considered individual which reflects the possibility for threats to be multiplied if same attack concerns different components. This possible multiplication of threats is processed with event matrix analysis. It can be done, because the threats are considered equal to each other. Only distinction is the probability of the occurrence, not the severity of the possible damages. The risk probability is defined in (1), where $prob_i$ is the likelihood that threat numbered as i occurs, n is the number of faults (i=1 to n), c_i is cost to reduce threat vulnerability i by 1 % point, d_i represents damages incurred by threat i.

$$r_i = prob_i - (c_i / d_i) * (Slack / \sum_{i=1}^{n} c_i^2 / d_i) \quad (1)$$

Slack represents the shortfall in funding (2) with the budget total M. If this shortfall is greater than zero, it must be spread across n threats.

$$Slack = \sum_{i=1}^{n} c_i * prob_i - M \quad (2)$$

With resource optimization, Lewis presents allocation formula (3) where r_i is the amount of reduction in risk i obtained by investment $alloc_i$ (portion of budget M allocated to remedy threat i).

$$alloc_i = c_i * r_i \text{ , for all } i = 1 \text{ to } n \text{ threats.} \quad (3)$$

The equations above answers to question, how much it costs to improve the security with one relative percentage on one single threat. It considers the attack probability reduction in one component.

As we stated before the vulnerability analysis has been considered very important method in military context. It has been considered a methodology with which a vulnerable targets can be identified and start preventive actions against threats. It guides the process management as well as the system software that is built to support it. With dynamic high security environments, it improves the awareness of the current security level [18]. However the challenge has been the computing resources needed to analyze the constantly changing environment and to address the sufficient amount of security with limited resources. In next chapter we propose a set of properties to be applied with vulnerability analysis technology. With them, we can identify the components or parts of the system to be secured more in order to use budget effectively.

3 Vulnerability Analysis Conducted by Business Resilience

Cyber attacks or cyber warfare are very popular topics on today media. Focus in these discussions lie usually on who is the perpetrator, what kind of attack is performed and how the attack could have been prevented. Especially the last topic can be a center of interest for long after attack or incident itself has ended. Duration of the discussion can be long particularly, if the attack has caused inconvenience for lots of people. The problem of this kind of discussion is that it usually concentrates on reactive actions and technological details of attack prevention. The discussion can be inconvenient to business being targeted and such vivid discussion can be one of the original goals of the malicious actor. It is typical, that little attention is paid for the real damage the attack really causes and why the systems should be protected in the first place. The consequence of the technical related discussion is, that the future security improvement investments for the systems of targeted corporation are possibly exaggerated and only against limited and media aware types of attacks.

Despite the public discussion, it is widely known that the systems cannot be secured fully against attacks. The more system is tried to be secured, the more it costs. Actually investment costs increase exponentially in relation to achieved protection of the overall system. Systems which have little or none protection can be more secured with little invest. Similarly, to improve overall security in a high security system requires typically significant investments.

Moreover, it shall not to be forgotten what the system is protected for. The implementation technology, how the possible attack is conducted or the cyber war is never a reason itself for improving the system security. Systems have always reason for existence which is determined by the use in business. The criticality of the system is directly related to the how crucial system is for the business and how little failures of the system can be avoided without compromising the business. This means that the significance of the system must be evaluated by the business impact caused by compromised knowledge, compromised sensitive personal information, system outage or failure. Moreover the type of damage for business must also be noted and taken into consideration. Cyber threats can cause enormous direct and indirect damages. Interruption of business operations causes loss of revenue and income. Recovery of operations can cause expenses for a significant amount of time, even for several years. Reputation loss causes direct and indirect expenses. Cyber attack may cause legal fees, fines and/or sanctions. Loss of immaterial capital, such as research and development investment, will cause expected cash flow reduction. Exposure of sensitive business of customer data will cause direct and indirect expenses as well as reduction of cash flow and reputation loss.

We propose a concept called Business Resilience to determine this tolerance for system security. We define the concept of Business Resilience as ability for business to survive after immaterial and material capital loss due to significant parts of the information system environment are paralyzed or exposed to open public because of a cyber attack or collateral damage in cyber environment. With business resilience we can determine comprehensive improvement of the tolerance against risks for organization. Main goal of this determination is to gain sufficient security level against identified threats with resources available.

3.1 Properties of Business Resilience

The properties to determine information security, sustainability and evaluation of Business Resilience in certain system are listed in Tables I and II. The Business Resilience is quantified by the financial key ratios of the business. We have limited the balance sheet values from this paper in order to maintain the simplicity and yet comprehensive model. For sufficient approximation at least key ratios revenue and cash flow must be observed. The limit of resilience defines in financial value that the business can tolerate in direct losses during an attack. In other words, it answers to the questions how long a business can remain unavailable and how much expenses corporate afford to recovery actions before bankruptcy. The reputation means the business reputation which might be lost because of the unsuccessful prevention of the attack or publicity of the exposed contents. It might cause the loss of trustworthiness of the business customer avoidance in the markets. The reputation can be determined as a financial value function over time. It means that the value of reputation loss changes over time. At first reputation loss of the corporation will be high when an attack and vulnerabilities of the system are published to media. With successful countermeasures and prevention of the increased damages the value for reputation losses are limited. On the other hand, if the succession of an attack is continuous, sensitive data is leaked to open public or the prevention of the attack

fails, the reputation losses increases. We assume that this continuous function represents the situation that the attack continues and prevention fails. Naturally, the value of reputation loss can be reduced by carefully planned information delivery for public.

The business resilience is financial tolerance of the components that are compromised. At business level the collection of business components are as a property. Properties for each component are described in Table II.

To avoid and decrease the losses of a cyber attack the risk can be transferred of shared. The risk transfer is directed to component. In business context total amount of transferred risk is the sum of all transferred risk in components. It is notable that for example insurance against cyber attack is a component in this model. Nevertheless the insurance component is in use, it is exceptional that the corporate could transfer risks entirely. Naturally all of the risks cannot be avoided. Residual risk must be accepted. The determination of the quantity for the residual risk is challenging to evaluate. A suitable approximation is achieved by analyzing and forecasting the possible change in cash flow due to cyber attack. In our model it can be calculated by summarizing the lost revenue of all components compromised by the attack and comparing it to the corporate cash flow. When limit of resilience equals to total lost revenue subtracted by the remaining cash flow the continuity of the business has become endangered.

The last property for Business level is the investment budget that can be used to improve the information security. This property determines the possibilities for improving tolerance against cyber attacks. The technique for determining how the investment can be optimized and allocated to different components is discussed in chapter 3.2.

Table I. Properties of Business Resilience in overall system

Property	Value type	Description
Revenue	Financial value	Key ratio on the income statement
Cash flow	Financial value	Key ratio on the income statement
Limit of Resilience	Financial value	The limit of losses that can be tolerated before bankruptcy.
Reputation Loss	Function of Financial value over time.	Estimated value of the reputation loss due to an attack.
Business Components	Array of components	Individual component properties are described in Table II
Total transferred risk	Financial value	The total amount of transferred or shared risk.
Information Security Investment Budget		Investment Budget for Information Security improvement.

In table II we describe the properties of each business critical component. The component will have a short description of the role and the meaning for the business. Business criticality is the numeral value of the criticality for business. The method for determining the business criticality is described in chapter 3.2.

Table II. Properties of Business Resilience for each component

Property	Value type	Description
Component description	String description	Component name, description and role in system.
Business Criticality	Normalized value [0..1]	Criticality of the component in relation to business.
Cost of Investment	Financial value	Development costs of the component.
Estimated Lost Revenue	Financial value	Expected direct costs if the component is not available due to an attack.
Recovery costs	Financial value	Estimated cost for the recovery of the component.
Immaterial Properties	Financial value	Estimated value of business advantage in relation to competitors. Value of immaterial capital that is bound to component.
Sensitive data content	Financial value	Estimated value of the business confidential data which is on components responsibility.
Customer data content	Financial value	Estimated value of the confidential customer data which is on components responsibility.
Risk	Probability	Estimated risk that any of the identified threats will success and cause component unavailable.
Threats	Array of identified threats	Identified threats towards the component with probability of attack succession and cost of probability reduction by one percetage.
Minimum cost of security improvement	Financial value	The minimum cost for risk reduction by one percentage.
Transferred risk	Financial value	The amount of transferred or shared risk of the component.

Business operation is the downtime of the business and the loss of revenue in all lost business operations because unavailability of the component. Immaterial capital such as patents and IPR:s are the value for distinctive properties in the markets (for example the business secrets that gives the advantage towards the competitors). Customer data loss is the value of the lost, corrupted or exposed customer data. This data is business secret as well as it might be sensitive such as personal information or credit card data. Sensitive data is the data contents of the system which has some business value (for example the results of some experiments or the cost prices of the products).

Success probability on threat in each component of the system may vary and the real cost what threat produces is its impact and damage to all influenced components. This dictates that investing with financial minimums, the threats to the system must be considered and to be decided what kind of real risk we are able or willing to acknowledge. We state, that the probability of successful attack against

business resilience is the probability of a threat succeeding in any component as presented in (4) where Fi is the set of components that are influenced by the threat i. Fi = {compj}, where the system component j is influenced by the threat i. Therefore P(Fi compj) denotes the probability for succession of an attack on component by certain threat i. We consider the threats to be nondependent to each other presenting individual threat in an attack.

$$P(\textit{threat } i) = P(Fi\ comp_1) + P(Fi\ comp_2) + \ldots + P(Fi\ comp_j) - P(Fi\ comp_1 + comp_2 + comp_j) \quad (4)$$

The risk function *R* represents the overall probability that some of the identified threats will succeed in system in some component. It is defined as (5)

$$R_n = f(P(\textit{threat}_{i1}), P(\textit{threat}_{i2}), P(\text{threat}_{ns})), \quad (5)$$

wherein *n* represents the total amount of threats and *s* the total amount of components. We simplify the above approach to represent it in more manageable form. We state, that it is sufficient to represent as a summation function where the risk R_j for component *j* is the sum of all probabilities of threats influencing that component, as in

$$R_n = \sum_{i=1}^{n} P(\textit{threat } i). \quad (6)$$

The collection of identified threats is connected to the component. Each threat has some probability for succession and evaluated cost of reducing the probability by one percentage. The calculation methods of the threats are discussed in more detail in chapter 3.3. On component level, the minimum cost of security enhancement can be determined by a minimum cost of security improvement as

$$\min(ci * R_i) = \min\left(\sum_{i=1}^{n} c_i * P(\textit{threat } i)\right), \quad (7)$$

where $i \in [1, n]$. Risk can be transferred by the contracts for example to the service provider, customer, and subcontractor or to insurance company.

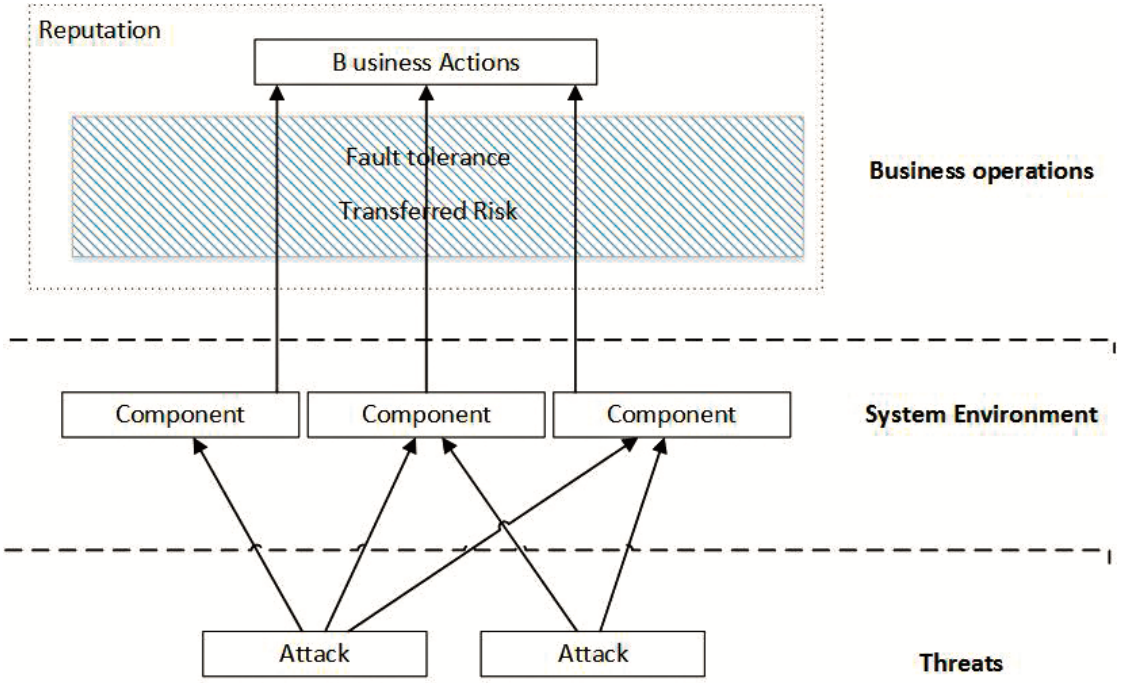


Figure 1. Logical illustration for the relations of business resilience, components and Threats.

In Fig.1 the relation of business resilience towards components and threats is presented. The arcs from attacks to component illustrate the risk that successful attack presents and the arcs from components to business operations describe the criticality of the component. The weight of the arcs can define the relativeness among other arcs. The business resilience here is the tolerance for faults during outage of component within successful attack. The risk of outage can be transferred which enhances the business resilience. The reputation illustrates the business operations that are reviewed by the public.

On next chapter we describe a simple method for determining the criticality of component. It is an approximation of the subjective interpretation of the strategy, but it allow corporate to focus limited investment budget to most crucial components.

3.2 Determining the component criticality

As stated before, we argue that the reduction of the optimal risk level or the probability of the critical point in system is relevant only when it is reasonable for overall environment. To evaluate the reasonability we propose a simplified way to quantify the criticality. Attributes that determine the business criticality for each component are listed in Table III. Value for determining the business criticality to be applied in each component can be found from the properties of the component (Table II). The good convention to determine the whole system is to proceed from top to down, to start with larger parts and break down into more detailed components. It assists in focusing the relevant information. Within Table III can be seen, that that different kind of attacks have different kind of financial impacts. Investment value is the financial value of the component and can be considered to be lost because of an attack. This refers the payback time of the investment

calculations which are not to be actualized. Value of lost revenue is the immediate financial damage and the impact of an attack. Recovery expenses are the costs that are actualized in order to restore the level before the attack. The value here is not considering the timeline of the recovery. Recovery costs can be also caused by replacement of the component. With immaterial impact, the value of the lost component can be considered as the amount of investment or with unpublished patents the loss of future productivity or income.

We determine overall criticality of the component by normalizing the summarization of lost expenses v (investment value, lost revenue, recovery expenses) from component. In normalization the most critical component is valued to 1 and the rest by the relative value to the maximum value. We do not consider the security enhancements to a component as investments. That is, the value of a component in relation to business resilience does not increase by investing to safety measures. This is because the cost of outage does not change directly. However, the recovery time or expenses might alter due to security investment and that also changes the criticality of the component. Criticality of component C_j is represented by

$$C_j = v_j \,/\, \max(v_j), \tag{8}$$

where $j \in [1, S]$ and S indicates the set of components in system.

Table III. Matrix of attributes that determine component criticality.

Impact	Investement value	Value of lost revenue	Recovery expenses
Business operation		x	x
Immaterial capital	x	x	
Customer data		x	x
Sensitive business data		x	x

Multiplying the criticality property of a component with the risk for component (6), we can prioritize the component improvement urgency. The closer the multiplication approaches to 1, the more urgent the improvement is.

3.3 Characteristics of Business Resilience

In this chapter we examine the characteristics of Business Resilience in more detail and present approaches how the information security investment can be most profitable. We alter the approach Lewis presented in model based vulnerability analysis from the threats to the components, because as we have stated, the components are the units that ensure business continuity. Instead of focusing individual threats on improving the protection of the system, we consider the component itself to be improved. In practice, instead of estimating the costs of the countermeasures against one threat, we consider the cost of the better component or the continuity of the system after attack.

Continuing with business resilience approach, the cumulative impact of the threat can also be treated. In large attacks, one threat vector affects to multiple components. On the other hand some of the large attacks may cause limited or none damage in one component in relation to business continuity. Usually it is too expensive to build preventive mechanism to each component separately against the attack, while the costs of the attack are limited to small proportion of the expenses. In that case we can approve the risk. But more importantly the threat must be analyzed to the business damage it causes. In that way we cannot bypass the affected components by the attack. The real financial damage of a single attack is the sum of all damaged components and their cumulative costs.

We propose that the distinction of the threat is always the actual impact to business which differs from the original model presented by Lewis. This fact emphasizes the business resilience approach and those components that are most essential to business continuity are improved first with enhanced protection against attacks.

With business resilience approach the criticality property of the component is emphasized. We agree with Fung et al. that in entirety of the system is as strong as the weakest link [19]. Moreover we assume, that the systems should be always being protected against common and known general attacks, and that the malicious actors behave economical way as well. Fung et al. proposed also a difficulty level in their attack model which stated, that attackers tend to find the easiest way, the one that needs least effort to be exact, to have the greatest damage in certain attack type[19]. Moreover, the probability of the successful attack is not as relevant as the damage, because we can be sure that in general there are malicious actors more that we can prevent our system to be prevented from. Consequently, the weakest components in relation to the business resilience must be fixed first. The mathematical downside of this approach is, that the most probable and expensive threats might stay with inadequate level of security and we approve that some attacks may occur. However we argue, that the criticality factor will take care that the most fundamental and crucial threats are taken sufficiently into consideration. And like we stated already before, the systems cannot ever be built to be entirely attack safe.

Business resilience of the system determines if all business relevant components of the system are unavailable, the business will be over after certain time. The relative portion of the resilience *PR* determined by a component can be evaluated by the values of all components as

$$PR_j = v_j \,/\, \sum {}^{s}{}_{j=i} \, (v_j), \tag{9}$$

where *s* indicates the amount of components in system. Total sum of all component values must be always smaller than the business resilience. Otherwise single attack can damage irrevocably operative business or reputation of the organization. In public authority this means that the credibility of the authority can be questioned and the safety of citizens are compromised. The means to improve the overall resilience of the system can be made by the insurance or improving the information security of selected or all components. On latter case the simplest approach on improving the system is to apply (7) to single component. However, this approach

relies on local optimization and the instant improvements of limited financial resources. Improving one component does not necessary give protection against threat at large. That is why threat must be solved collectively on all components it affects.

The total financial value of a threat towards our system can be calculated by summarizing the component values that are impacted by the threat on succession. We simplify the calculation to emphasize the threat value determining that with successful attack, all components that are influenced by successful attack are summarized to total value v_i, as (10)

$$v_i = \sum F_{vi}, \tag{10}$$

wherein F_i contains all the components influenced by the threat and v represents the value of the component on the set. In order to determine vicinity for the value of threat we compare it to the entire business resilience BR of the system as relative value of threat RV_i

$$RV_i = v_i / BR \tag{11}$$

Security actions should take place, if total value of threat is approaching to business resilience value (ie. $RV_i \approx 1$). We also argue that if the attack succession probability of threat is greater or equal to the relative value of threat, the threat should be considered as a risk and action plan to avoid the risk need to be composed.

The alteration in system affects always to the vulnerability composition, threat set with probabilities and the role of each component in overall system. That is why after every change on components the evaluation on the vulnerability must be done again. The methodology Lewis presented is comprehensive, yet too heavy to real time analysis on dynamic environment. We propose a modified attack tree approach to solve this challenge. It is described in more detail on next chapter.

4 Real-Time Vulnerability Analysis in Dynamic Environment

In dynamic high security environment it is impossible constantly to perform all steps from scratch that are carried in critical infrastructure protection and described in previous chapters. We present a lighter and more computative method that can be executed after different kind of changes in set of components. These changes include improvement and the reduction on security of the component, new components in the overall system (for example new nodes to network) and disabling some components from the network (for example if they are compromised in attack). We extend the attack tree methodology presented by Fung and Hung [8]. The attack tree methodology is developed to work in distributed SOA (Service Oriented Architecture) environment where services are employed to fulfill a system objective [8]. In our military context services are component of the system environment and can be considered as services, network nodes or critical systems.

In next chapter we observe how the business resilience properties are handled with the changing environment.

4.1 The Impact of Business Resilience to Intrusion Modelling

In Attack tree methodology, system will be inspected by the attacker aspect. The succession of the attack is the succession of top level goal [19]. AND –operation implies that all branches of the tree must be succeeded in order to succeed in attack and cause the system to fail [19]. The most cost effective way to improve the total security in AND -operation is to improve the security in branch where the improvement is cheapest. Similarly OR-operation implies, that only one of the branches in OR –operation must succeed in order to succeed in attack [19]. It also means that to improve the overall information security, the security level must be improved in every branch of OR-operation.

In dynamic environment the vulnerability setting of the system can change rapidly due to intrusion or executed countermeasure. We combine the dynamic construction of high security environment to an automatic and constant vulnerability analysis. We utilize the business resilience properties in AND-, OR – and LEAF operations presented by Fung and Hung [8]. By this we achieve a more survivable and resilient environment against the attacks or damages. In Fig. 2 the sample attack tree construction in relation to process diagram is presented.

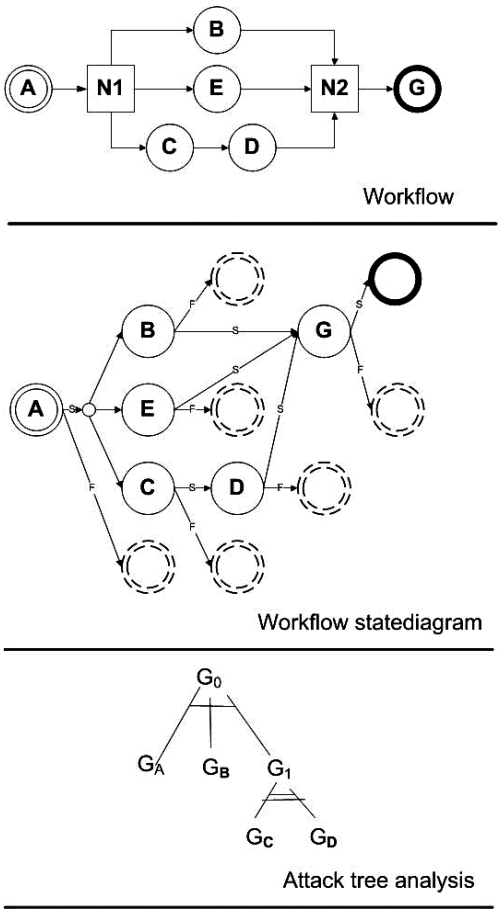


Figure 2. Sample attack tree construction from workflow [19].

We need to be aware the resilience level of the environment after the change. We present four algorithms for modelling the change in business resilience: Initialization, resilience change in a component, adding a new component to system and excluding a component from a system. For awareness of the security performance, it is relevant to identify the location of the new component and what is the influence to the resilience of neighboring components. On the leaf level there is a single operation or a component which failure has an impact to the system execution. Leaf is the level that you can address the costs and impacts. The higher levels of tree are decreasing of increasing the total resilience depending on the operation.

Algorithm 1. Algorithm to initially identify the resilience level

First round with all Leaves

Calculate component risk
Calculate component value

If component value > current maxvalue then
maxvalue = component value

Second round with all leaves and nodes recursively

If node is LEAF
Calculate criticality with maxvalue
Calculate improvementUrgency = risk * criticality
if improvementUrgency > current maxImprovementUrgency then
maxImprovementUrgency = component improvementUrgency

If parenting node is AND –operation
node value = max(value of direct descendants)
node risk = max(risk of direct descendants)
node criticality = max(criticality of direct descendants)

If parenting node is OR –operation
node value = sum(values of direct descendants)
node risk = sum(risks of direct descendants)
node criticalities = sum(criticalities of direct descendants)

The computational cost of calculation is at most $3n(n+1)$, where n is a total amount of leaves. In practice this means that there are always at most two leaves as siblings. As we can see, the cost is polynomial and to decrease the computative power needed on real-time to this analysis, we suggest that the initial baseline for the resilience is calculated first. It can be made for example on Lewis model step three where the fault tree is built.

Algorithm 2. Algorithm for determination of resilience after addition of a component

The added component is always a leaf. It is assumed that the parent of added component is not a leaf. It should be determined how the component is added to system, ie. through AND- or OR- operation.

With added component

Calculate component risk
Calculate component value

If component value > current maxvalue then
maxvalue = component value
set maxValueIsChanged to true
Calculate criticality with maxvalue
Calculate improvementUrgency = risk * criticality

if improvementUrgency > current maxImprovementUrgency then
maxImprovementUrgency = component improvementUrgency

If maxValueisChanged = true then
For each LEAF calculate criticality and improvementUrgency
For each parenting node calculate properties similarly in initialization phase.
else
With all parents of added component

If parenting node is AND –operation
node value = max(value of direct descendants)
node risk = max(risk of direct descendants)
node criticality = max(criticality of direct descendants)

If parenting node is OR –operation
node value = sum(values of direct descendants)
node risk = sum(risks of direct descendants)
node criticalities = sum(criticalities of direct descendants)

It is noteworthy, that calculating the risk to added component can impact the total probability values of the threat. In other words, the addition of a component can have significant changes to overall system and re-evaluating the whole system analysis can be justifiable.

Algorithm 3. Algorithm for determination of resilience after excluding a component

With all parents of excluded component
If excluded node has one sibling node then
Exclude parent node and attach sibling to the parent of parent

If parenting node is AND –operation
node value = max(value of direct descendants)
node risk = max(risk of direct descendants)
node criticality = max(criticality of direct descendants)

If parenting node is OR –operation
node value = sum(values of direct descendants)
node risk = sum(risks of direct descendants)
node criticalities = sum(criticalities of direct descendants)

The value of excluded node can contain the maximum value of the system. However it is not necessary to calculate the whole system at this point, because relative criticalities still remain. We argue that excluding components are caused by an attack and after recovery components are added again to the system. The max values are calculated during the additions of the system. We encourage that one component should not be overvalued compared to overall system and new components added to system should not exceed the max value of previous components.

Algorithm 4. Algorithm for determination of resilience after change in survivability of a component

With altered component
Calculate component risk
Calculate criticality by with maxvalue
Calculate improvementUrgency = risk * criticality
if improvementUrgency > current maxImprovementUrgency then maxImprovementUrgency = component improvementUrgency

With all parents of altered component
If parenting node is AND –operation
node risk = max(risk of direct descendants)
node criticality = max(criticality of direct descendants)

If parenting node is OR –operation
node risk = sum(risks of direct descendants)
node criticalities = sum(criticalities of direct descendants)

Restructuring the tree can be completed by adding and excluding nodes and leaves appropriately. We argue that the algorithms presented are suitable for dynamic environment, because change, addition and exclusion of a component need at most $3k$ operations where the k is the level of hierarchy for the processed component. In those rare situations that addition changes the existing maximum value of all

components, the criticalities in whole system need to calculated again. This does not happen in normal operative execution, but in significant change in system. At that time the analysis should be re-evaluated in every case. With presented algorithms we gain the most important properties of the system for the two top levels. Properties are total resilience value, risk and criticality for portion or collection of components of a system.

When improving survivability of the system, it is most convenient to have AND - operations in critical components [19]. In practice it means that component services should be coupled. It can be expensive to build backup systems to every operation in large scale environment. However in high security systems, it is necessary that the compromised component or system segment can be turned off. This exclusion of damaged or compromised component guarantees the operability though with limited resources.

5 Future work

We find the next step is implementing the real-time vulnerability analysis and resilience determination algorithms to high secure cloud environment. We have planned to improve the algorithms by expanding them with system recovery features in order to improve the survivability of a system. The survivability of the system and the overall information security against certain types of attacks can be improved cost effectively by having attacking tools in countermeasure selection available. It means that ability of diminishing or eliminating the source of the threat is less expensive than building exaggerated and oversized security mechanisms. This approach changes the formulation of the vulnerability analysis from purely defensive view to more active defense.

Another track under research is to have these survivability enhancements deployed into software development process seamlessly. The advantage of this is, that the costs of building security mechanisms to the system at construction phase is significantly less than adding them to completed system which is already in production.

6 Conclusions

In this paper we examined the vulnerability analysis within the military context. We stated that the improvement of information security must be considered by the properties of the business resilience. We identified the properties of business resilience and examined their determination and how they interact to overall environment. With the properties we are able to process direct and indirect costs of component for business when they are not in use. In addition, properties consider also immaterial expenses as enablement for future business. We presented quite comprehensive set of analysis tools for determining the risk of threat to our business and for allocation of the resources to components that are most vulnerable from the view of resilience.

With real-time vulnerability analysis in dynamic environment, we facilitate the usage of business resilience properties in dynamic construction of high security environment. We also achieve an awareness of information security level after recovery from an attack or after security enhancement of a system. We have limited the observations how to detect malicious attacks or how the component security is enhanced, but we presented algorithms to determine overall business resilience of the system after such events. With presented methodologies we can identify the vulnerabilities of the system in relation to business resilience, we can evaluate what we can achieve with the enhancements of the system and lastly we are able to allocate limited resources to most vulnerability components in order to gain best protection to identified threats.

Acknowledgements

This work has been partially supported by CGI in Finland (http://www.CGI.com/) especially by Jan Mickos. Jan Mickos contribution in determining the concept of business resilience is appreciated.

References

[1] M. Barbacci, "Survivability in the age of vulnerable systems", IEEE Computer, 29, 11(1996), page 8.

[2] S. Hariri, G. Qu, T. Dharmagadda, M. Ramkishore, and C. S. Raghavendra, "Impact Analysis of Faults and Attacks in Large-Scale Networks", IEEE Security & Privacy, pp.49-54, 2003.

[3] S. Jajodia, S. Noel and B. O'Berry, "Topological Analysis of Network Attack Vulnerability", Managing Cyber Threats, Massive Computing Volume 5, 2005, Springer US, pp.247-266.

[4] Y. Li, H. Yang and K. Xie, "Network Node Importance Measurement Method Based on Vulnerability Analysis", Proceedings of the 4th International Conference on Computer Engineering and Networks, 2015, Springer International Publishing, pp.1281-1289.

[5] Y. Zeng and R. Xiao, "A networked approach to dynamic analysis of social system vulnerability", Journal of Intelligent and Fuzzy Systems, Vol.28, No.1, 2015, pp.189-197.

[6] E. Jenelius and L. Mattsson, "Road network vulnerability analysis: Conceptualization, implementation and application", Computers, Environment and Urban Systems, Vol. 49, January 2015, pp.136-147.

[7] H. Lv, Y. Zhang, R. Wang and J. Wang, "Graph-Based Real-Time Security Threats Awareness and Analysis in Enterprise LAN", LISS 2013, Springer Berlin Heidelberg, pp 1299-1304.

[8] C.K. Fung and P.C.K. Hung, "System recovery through dynamic regeneration of workflow specification", Proceedings of the Eighth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, Washington, DC, 2005, pp149-157.

[9] P. Kumar and S. B. Singh, "Fuzzy Fault Tree Analysis using Level (λ, ρ) Interval-Valued Fuzzy Numbers", Mathematical Theory and Modeling, Vol.5, No.2, 2015.

[10] E. Bozdag, U. Asan, A. Soyer and S. Serdarasan, "Risk prioritization in Failure Mode and Effects Analysis using interval type-2 fuzzy sets", Expert Systems with Applications, Volume 42, Issue 8, 15 May 2015, pp.4000-4015.

[11] N. Mead, R. Ellison, R. Linger, T. Longstaff and J. McHugh, "Survivability Network Analysis Method", CMU/SEI-2000-TR-013, September 2000.

[12] A. Moore, R. Ellison and R. Linger, "Attack Modeling for Information Security and Survivability". CMU/SEI-2001-TN-001, March 2001.

[13] J. Cardoso, Z. Luo, J.A. Miller, A.P. Sheth and K.J. Kochut, "Survivability architecture for workflow management systems", Proceedings of the 39th Annual ACM Southeast Conference (ACM-SE'01), Athens, Georgia, May 2001, pp 207-214.

[14] T.G. Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Wiley-Interscience, 2006.

[15] J. Newsome and D. X. Song, "Dynamic taint analysis for automatic detection, analysis, and signaturegeneration of exploits on commodity software", In Network and Distributed System Security Symposium (NDSS), San Diego, February 2005.

[16] M. G. Kang, S. McCamant, P. Poosankam and D. Song, "DTA++: Dynamic Taint Analysis with Targeted Control-Flow Propagation", NDSS. February 2011.

[17] H. Adrian, and B. Cheney, "JMD: A Hybrid Approach for Detecting Java Malware", Proceedings of the 13th Australasian Information Security Conference (AISC 2015). Vol. 27. 2015.

[18] K. Zaerens and J. Mannonen, "Concept for the Construction of High Security Environment in Public Authority Cloud", Lecture Notes in Electrical Engineering, Springer-Verlag, pp. 401-408, September 2012.

[19] C. Fung, Y. Chen, X. Wang, J. Lee, R. Tarquini and M. Anderson, "Survivability analysis of distributed systems using attack tree methodology", Military Communications Conference, 2005, pp. 583 – 589.

Providing a Tactical Domain For an Independent Nations Task Force

Stuart Marsden
Finnish National Defence University
stuartmarsden@finmars.co.uk

Abstract

Any independent sovereign nation will wish to ensure that their land forces are equipped to protect that nations interests. Technology for Command, Control, Communications, Computers, & Intelligence (C4I) systems is advancing rapidly and even smaller nations must keep up. This paper looks at the types of considerations when planning and equipping a task force from the soldier platform to the upper tactical echelon. The paper will consider some of the key technology enablers that can deliver operational benefit. An architectural approach is given that will allow the right equipment to be used depending on the situation. This approach is demonstrated by 4 example architectures for different military scenarios. An acquisition approach will be proposed to ensure freedom, flexibility and value for money. Interoperability and other not material development areas will be considered.

Keywords

C4I, tactical, communications, acquisition

Paper type

Research paper

1. Introduction

As we look towards future military equipment and ways of working there are many aspects that must be considered. Technology drives much of the advancements but does not by itself deliver the operational benefits and capabilities that are required. It is important to consider all the development lines used in the US Joint Capabilities Integration and Development System (JCIDS, 2012): Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTmLPF-P). Whilst this paper concentrates on the Materiel or Technology any architecture and system must be implemented in a framework that delivers a complete system.

The topic has been approached in the context of an independent tactical force and starts from the soldier/platform level to the upper tactical echelon. As an example this would be a Brigade size force with armoured, mounted and dismounted elements. This would include organic artillery, engineer, signals and logistic support. In addition they would have attached air and naval assets and a Special Forces (SF) component.

The Area of Operations is considered to be in the defence of the home nation. However, flexibility is retained as a key requirement and no assumption is made about fixed communications infrastructure. The proposed technologies are therefore applicable for more expeditionary operations.

The time frame for the new capability is 2035. The various technologies will however mature at different rates and could be ready much earlier for insertion in to a legacy system. This will be covered later when considering a transition plan.

Whatever the time frame some limitations will remain. Size Weight and Power (SWaP) requirements especially for the dismounted soldier are going to cause constraints. Access to the electromagnetic spectrum will remain finite and contested by other users and the enemy. Some of the technologies assessed may work more efficiently within these constraints.

This paper assesses some of the technology areas in the first two sections divided in to communications and the application layer / software infrastructure. In the next section an architectural approach is proposed with examples in the following section. The paper then puts the system issues in context of other lines of development before concluding and suggesting future work.

2. Communications

Networks with the ability to pass data and voice are already common in the military domain. However, at the lowest tactical level the access to high throughput data which is connected to a larger tactical internet is not ubiquitous. New equipment such as Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) and biometrics demand a data rate that is not currently available. Some technologies which can help to close this gap are:

Software Defined Radio (SDR). In the same way that a general purpose computer can run different software applications, a SDR can be reprogrammed to have different waveforms and frequencies.

Mobile Ad-hoc Networks (MANET). These networks are able to form networks and allow data to travel between each radio and 'hop' across multiple radios.

Cognitive Radios. These radios are more intelligent in their use of the electromagnetic spectrum. They can detect where a clear channel is available and use it possibly multiplexing many different channels to increase throughput.

Software Defined Networks (SDN). Enabling the inter connectivity of heterogeneous networks is a skilled job which often requires proprietary knowledge of different network equipment. SDN address these problems by allowing dynamic and standardised ability to monitor and configure networks.

Software Defined Voice Networks (SDVN). All informed voice remains the most common method of command and control in dismounted forces. SDVN allow voice to run on top of data and thus voice networks can be defined dynamically.

2.1 Software Defined Radio

SDR has the potential to make the selection, upgrade and operation of military radios more flexible. In the same way that a Personal Computer (PC) allows the selection and use of software to suit an operation, a SDR could allow flexibility (Mitola, 1995). The Software Communications Architecture (SCA) was born out of the Joint Tactical Radio System programme and provides a standard framework to describe radio waveforms (Bard and Kovarik, 2007). For an independent nation the benefits of SDR could be marginal, as using an SDR to run only one set waveform delivers no benefit. For a coalition the ability to share a waveform and communicating directly can be desirable for latency and ease of interoperability. The security considerations however may preclude such a direct connection. An SDR could have the benefit of allowing a suite of waveforms to be selected depending on the frequency or the type of communication (satellite, terrestrial or ground to air) (Vankka, 2005). A non SDR also gives this possibility but does not allow a waveform to be added after the radio has been purchased.

The waveforms in the military space remain proprietary and vendor-specific. It is possible that by 2035 they will have become more commoditised and generally available in the same way that cellular standards are published openly. At this point SDR has not delivered the hoped for benefits and programs such as JTRS have had limited success (Goeller & Tate, 2014). SDR could allow the addition of active Combat Identification to a more standard waveform. The radio could monitor an interrogation frequency at set time frames and respond when targeted by Air or other assets.

2.2 MANET

MANET allow networks to be formed at the lower tactical level without detailed engineering. They use different approaches to sharing routing information but with the same goal of allowing data packets to be passed across the network (Royer. & Chai-Keong, 1999). Whilst MANET can impose its own issues on security, military variants have link encryption and added transmission security (Singh, Joshi & Singhal, 2013). MANET are already in service today but are restricted to the platform level. Soldier worn MANET data radios are just starting to appear but have limitations on range and must be incorporated to the wider tactical architecture to be fully usable. This is non-trivial for fully dismounted operations due to the need for a soldier-worn bridging node to a data backhaul. In mounted operations this is easier to achieve as the equipment can be carried and powered by the platform. This could lead to the requirement for a 'mother-ship' even in dismounted operations. This platform could be an autonomous robot or even an Unmanned Ariel Vehicle (UAV) which would have the added benefit of range and possible ISTAR functions.

2.3 Cognitive Radio

The lack of available spectrum is and will remain a key restriction in military communications. The current method of allocating chunks of spectrum is inflexible and inefficient (Akyildiz, et al., 2008). A more intelligent and dynamic way of using the spectrum could be enabled by cognitive radio (Mitola, Maguire, 1999). This

would maximise access to available spectrum and thus throughput whilst also simplifying battlespace spectrum management. There are no current true cognitive military radios but many MANET display similar properties, as a side effect of how they are implemented. Cognitive radios are being actively developed but the main barrier is procedural as spectrum managers need to progress from allocating chunks of spectrum for set times.

2.4 Software Defined Networks

As more complex and capable data networks begin to move in to the lower tactical echelons support becomes a problem. Signals trained soldiers with the required skills are not available at these levels and however, the soldiers have to concentrate on their primary role. MANETs go some way to abstracting complexity by forming mesh networks autonomously. However different equipments will tend to be linked by routers and need some element of configuration. This will be done prior to the commencement of operations but may have to be changed to reflect changing priorities. There needs to be a way to make these changes remotely and simply. SDN technology has the ability to do this and OpenFlow has become the open standard to implement (McKeown et al., 2008). It will allow remote monitoring/management and should be consistent across different equipment types. Current military communications systems have management software but it is often coupled to the manufacturer or system integrator. Insisting on SDN standards for network management can remove this restriction. The flexibility of OpenFlow can come at the cost of processing overhead and additional latency (Jarschel et al., 2011). Military networks do tend to have much more significant throughput and latency restrictions than OpenFlow may introduce and thus the flexibility becomes the key factor.

2.5 Software Defined Voice Networks

The use of all informed voice is integral to the command and control of tactical operations. Historically this has meant a dedicated radio (e.g HF, VHF, UHF) with a common frequency and, more recently, a shared cryptographic key for secure voice. In order to establish new voice network the radio and security key must be shared with the radio. Sometimes this can be done over the air but is often is often restricted by security requirements. This means having to physically move to each radio causing delays and risking lives. Generally one radio means one voice network and thus command vehicles requiring multiple radios and antennas.

As data communications become ubiquitous at the lower tactical levels another approach could address these concerns. Software Defined Voice Networks (SDVN) could allow voice networks to be abstracted on top of data. This is common place in telephony by the use of Voice over IP (VoIP) protocols (Ha & Yang, 2013). These underlying technologies can also be expanded to cover all informed voice. In the tactical domain the use of servers provides single points of failure due to enemy action, equipment failure or RF propagation. Therefore SDVNs need to be fault tolerant and distributed.

2.6 Commercial Off The Shelf

The military does not lead the way in communications any more with the mobile revolution having greatly advanced the state of the art (Hartman, Beacken, Bishop, Kelly, 2011). Military systems can save money and adapt more quickly by making use of Commercial Off The Shelf (COTS) technology. In communications the latest 4G standards offer large data rates, mobility and compatibility (Bhattacharyya & Bhattacharya, 2013). By 2035 this will have advanced further. A flexible military system will leverage these technologies but must be aware of the limitations. They were designed for the civil markets and do not have the same requirements as the military. For best utility a cellular system requires a dense network of base stations each with their own backhaul to the larger network. This is not available for early entry warfare but could possibly be established for defence of the home base or utilise the civilian infrastructure. In this case these key communications nodes would be vulnerable to attack by adversaries both kinetically and by cyber attack. The 4G standard does not have the same standard of security that is expected in military systems (Clancy, Norton, Lichtman, 2013). Whilst the security of the data can be layered on top of the network it is harder to add Communications Security (ComSec). These networks are thus vulnerable to spoofing and denial of service attacks.

COTS communications have established bands which are allocated throughout the world. These bands tend to be fully allocated and cannot be assumed to be available to the military in anything short of general war. In coalition operations there could also be multiple users trying to leverage the same technologies and frequency bands.

These limitations on the use of COTS technology can be mitigated with a number of approaches. The COTS technology can be militarised. The waveforms can be used adding additional ComSec. They could also be re-banded to more available military bands. Doing this adds to the cost and loses some flexibility but can get some of the benefits and remain more economical than technology developed purely for military use.

Cell based technology can be more widely utilised with the adoption of femtocell base stations. These can be fitted on platforms or part of the 'mothership' concept mentioned earlier. This would provide a local cell service usable by dismounts with standard smartphone type handsets. The range will be greatly reduced from a planned fixed base stations but depending on the type of warfare and terrain could cover a platoon or company size group. The femtocell will have to have its own MANET to connect in to a wider network. In more difficult terrain satellite connections could be used.

3. Application Layer and Software Infrastructure

The provided communications network gives the ability to share information between the required software applications. This will include Battle Management, Messaging, Chat, ISTAR and other special-to-arms applications. Whilst we can predict some of these applications, each different operation and task will have its own Information Exchange Requirements (IER). This in turn will lead to different

requirements and potentially new software applications. Coalitions also may require the use of new applications. The way that these applications communicate with each other is through protocols and data formats. Whilst standards do exist there can be many competing ones to choose from and they can be inconsistently implemented. Some key areas of software, protocols and formats that driving the design of the tactical architecture will be considered in this section.

3.1 Protocols

Applications communicate using protocols. There are several levels that these operate starting at the physical layer or Layer 1/2 in the OSI model (Zimmermann, 1980) which includes Ethernet and Wi-Fi up to the application layer (Layer 7). Adopting these standards makes communicating easier. At layer 4 we have Transport Control Protocol (TCP) and User Datagram Protocol (UDP). These protocols are at the heart of the modern network and universally supported. Most military data radios support TCP and UDP, however the choice of which can greatly affect the efficiency of the network.

TCP is a connection oriented protocol and positively establishes a connection before any data is sent (RFC792, 1981). TCP suffers from a number of well-known performance problems, which become more severe with longer delay, frequent errors, and large bandwidth (Vankka, 2013). UDP is generally more efficient on military networks as it is connectionless (RFC768, 1980). This saves a lot of overhead at the cost of the application layer having to ensure that a full message can be reconstructed. The packets can arrive in any order or not at all and the higher level protocol must deal with this unlike TCP where the network stack will ensure packets are presented in order and losses are re-requested..

Some military Information Technology (IT) systems use UDP only for messaging and have proprietary application level services dealing with these issues. Whilst there is no accepted standard in the tactical domain, there are standards based protocols which could be used in place of TCP. Stream Control Transmission Protocol (SCTP) (Stewart, 2007) is an alternative to TCP and UDP. It has been shown to be more efficient for transporting web services over military networks (Johnsen, Bloebaum, Avlesen, Spjelkavik, Vik, 2013). SCTP support is not universal in Operating Systems (OS) and network devices. The advantages of SCTP will vary depending on the underlying network implementation.

The intelligent selection of protocols can also make the most efficient use of the underlying network at the application layer. Many modern systems use the Hypertext Transport Protocol (HTTP) to transfer data. Web browsing relies on HTTP as does the Simple Object Access Protocol (SOAP) which is commonly used to deliver Service Oriented Architecture (SOA). HTTP is delivered on top of TCP and thus has disadvantages on tactical networks. Google is producing a complimentary protocol called Quick UDP Internet Connect (QUIC) (Carlucci, De Cicco & Mascolo, 2015). This allows HTTP type data to be transferred over UDP and by doing so allows data to be multiplexed more easily. This is important for wireless transfers such as MANET as it allows the packets to be concatenated into

larger frames for transmission. HTTP over TCP does not readily allow this as acknowledgement must first be received for a set window size of bytes. QUIC is not yet a standard but a sister protocol from Google for TCP called SPDY which has now been incorporated in to the recently released HTTP2 specification. In the assessed time-frame it is likely that QUIC or a successor will be more widely adopted.

3.2 Service Oriented Architecture

Enterprise architectures have made use of SOA for some time. It provides a level of abstraction and presents a common interface for the outside world. SOA architectures have only begun to be exploited in military computing at the strategic level of command (Zoughbi et al, 2011). The use of SOA in a more tactical environment is more challenging with near real time requirements and a restricted network (Saarelainen, Timonen, 2011). One key technology enabler for SOA is the Simple Object Access Protocol (SOAP). SOAP provides a standard way to describe and share information and services which allows different applications to connect without knowledge of the underlying data model.

SOAP can describe simple transactions and data but when dealing with more complex formats such as geographic information, they usually extend existing standards such as Geographic Markup Language (GML), Keyhole Markup Language (KML) or ESRI Shape files (Schnabel & Hurni, 2009). Applications used for Battle Management may support only a subset of these formats. Even with supported formats the implementation can vary which can potentially cause the data to lose fidelity. Therefore when using SOAP, data formats must be considered when selecting applications and for interoperability.

One way to resolve format issues and to structure information exchange is an Enterprise Service Bus (ESB) using a Publish/Subscribe model. An ESB provides another level of abstraction which among other things allows protocol conversion and data transformation (Chappell, 2004). This can consume data in multiple formats, normalise it, store it and send it on to subscribed applications. The Afghan Mission Network had such a service which was called the Publish and Subscribe (PaS) server. This concept has been taken forward and forms part of the Federated Mission Network concept (NATO Interoperability Standards and Profiles). An ESB is a complex software architecture but it provides flexibility and thus aids interoperability.

3.3 Semantic Web

One of the main benefits of an ESB approach is the ability to extract and search on semantic data. As the ESB ingests and normalises data it can hold it in a structured manner. It can then be drawn from multiple formats including human readable text. The data can be stored using the standard Resource Description Framework (RDF) and then searched using tools like SPARQL Protocol and RDF Query Language (SPARQL). This means other applications can understand and exploit it unambiguously based on shared ontologies. It also means that the ESB can be queried in a powerful way giving relevant results.

SOA and ESB provide many benefits but in the tactical domain can have severe drawbacks. If a central server was used then it could become a single point of failure and a bottle neck in the communications network. A tactical network should have system and geographic redundancy due to the effects of terrain and enemy action. SOA can be distributed across constrained networks and this can ensure access to information and remove pressure points from the data network (Ali, Hailong, Wei, 2013)

3.4 Applications

The choice of application will depend on the requirements and particular operation. This can change quickly due to the tactical environment or shared working with coalition partners. The key is to retain flexibility so that new applications can be incorporated quickly. This has proved difficult with monolithic C4 systems from defence vendors. As well as commercial lock in there are genuine concerns about system management and security when incorporating new software. Some mitigating techniques that can bring back flexibility are as follows:

Containerisation. Virtual Machines (VM) can be used to isolate instances of software but are quite a large overhead. A virtual machine runs a full OS and requires allocated memory and resources. This is possible especially when we consider Moore's law progress in the time-frame, however if each application has a full VM then this must be updated as well as the underlying OS. A lightweight modern solution is containerisation which uses the underlying OS but isolates the application environment (Dua, Raja, Kakadia, 2014). This means that applications and any dependencies can be updated without affecting others. It also keeps applications isolated so security concerns are reduced.

Open Source. The use of Open Source or Free Software can reduce costs when implementing a system but more importantly it provides greater freedom. If the source code is available then the system manager is not dependent on one vendor and their support. They also have the opportunity to analyse and improve the actual software. Whilst there is not a much military specific open source software use of standards based technologies discussed in this paper means that open source software can be adapted to the military need (Loechel, Mihelcic, Pickl, 2012).

4. Architectural approach

The above technology areas allow military requirements to be met but a system of systems approach is required to combine them to be a usable capability.

The combination of these technologies is best done in a 'golf bag' type approach. This allows the technology to be combined in a way that matches the environment and meets the commanders needs for an operation. So for example in a fixed environment a COTS cell based communications can be used and linked straight back in to the strategic system. For more dynamic high intensity warfare a more militarised MANET communications network can be used with satellite based reach back to strategic systems.

The required applications can be drawn from those already integrated and trained or a specialist application can be easily incorporated. The ESB means a new application can more easily draw data from the wider system. This also makes interoperability easier with the ESB being able to transform the data and send out on another protocol. This for example could enable Air Land integration by sending the ground picture out on Link 16/22. Business rules can be applied for information release so potentially the system could even interface with other governments or Non Governmental Organisations.

5. Candidate Architectures

To illustrate the architectural approach and how some of the discussed technologies can be utilised a number of scenarios are discussed. A brief description of the scenario will be given along with a candidate architecture that could be deployed.

5.1 Software Architecture

The software architecture remains the same for all the scenarios. As in Fig 1 the architecture is layered on top of the networks discussed below. A federated ESB will be established to allow sharing of information with redundancy. Standard external linkages such as to the Air and Sea Domain will be already integrated and provided by an ESB.

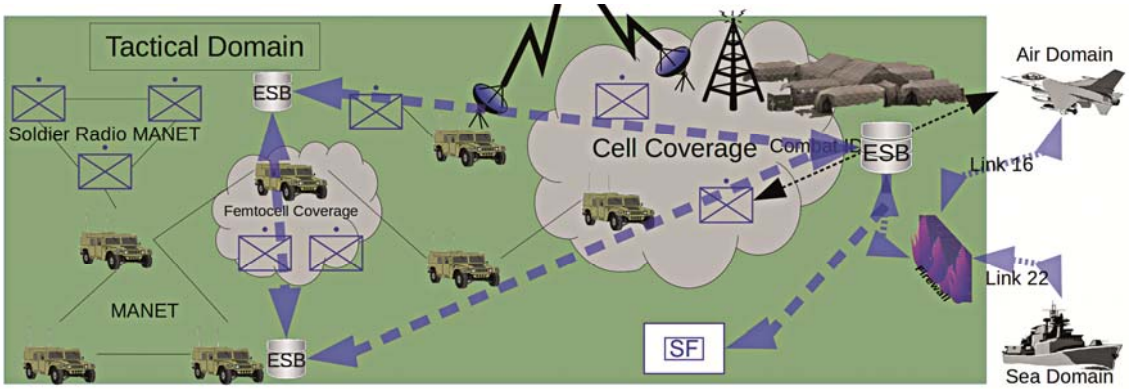


Figure 1. Candidate Architecture

5.2 Interoperability

Interoperability would be provided by the ESB in conjunction with firewalled touch points. The ESB will provide data normalisation to prevent unintended data leaking. The release of information can be implemented in the ESB by business rules or by positive release by a staff officer. Other external connections can be quickly specified and implemented using the ESB and a firewalled point of contact.

5.3 Protection of the home base from undeveloped adversaries

In this scenario operations are restricted to the countries own home base. The threat could be from subversive or state sponsored terrorists. The adversary does not have an advanced tecnological base but will make use of any available means to

create an effect. This architecture makes use of fixed infrastructure between the different headquarters and agencies (Fig 2). These will be wired links as part of the national infrastructure. Mobile units and temporary headquarters will be connected using a cell based infrastructure. This will be a combination of the nations safety networks which are presently usually based on Terrestrial Trunked Radio (TETRA) but in the time frame examined are likely to be a LTE or even 5G based safety networks. Where required capacity can be increased by using the civilian cell network. For those users in remote areas not covered by the cell network satellite means (both military and civilian) will be used.

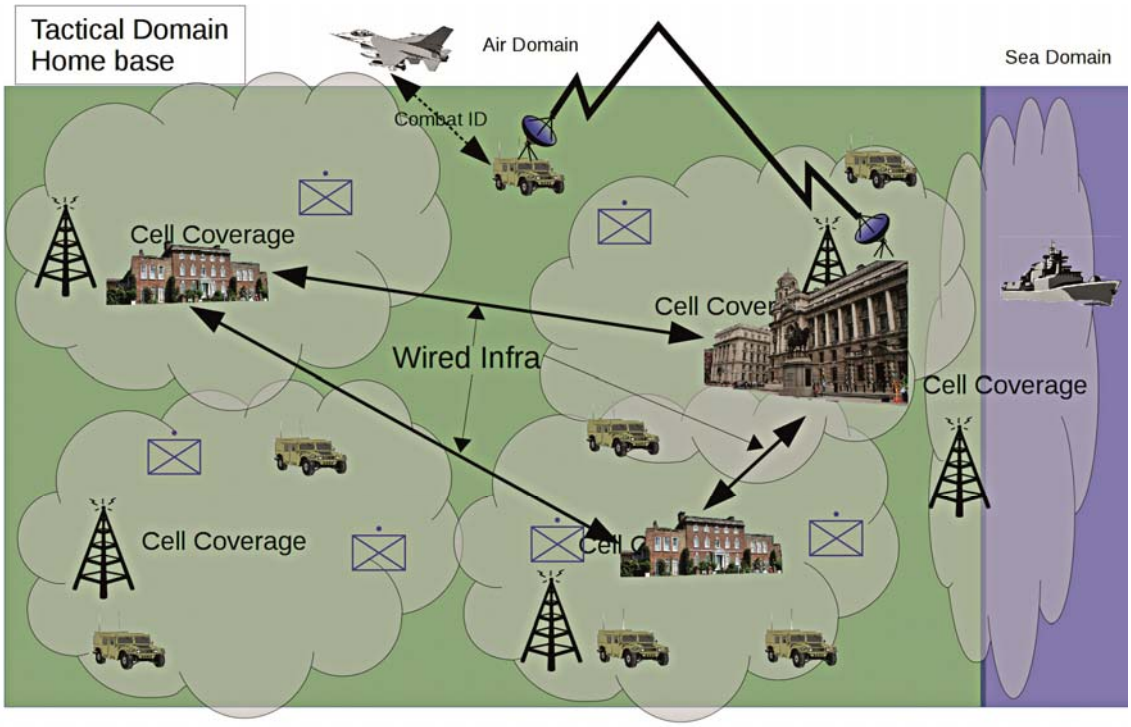


Figure 2. Protection of the home base from undeveloped adversaries

This network will be very capable in terms of throughput and connectivity. The user will access using the same systems they are used to during peace time. The reliance on fixed infrastructure however does make it vulnerable to attack. Even a technologically disadvantaged opponent can target cell towers and other network infrastructure. This means that physical security will have to be enhanced in these sites which will cost manpower and equipment. The use of standard infrastructure would allow supporters for the opponent to mount cyber attacks. State sponsors would likely have the ability to have an effect but also 'hacktivist' groups can use known vulnerabilities to impede the network.

5.4 Protection of the home base from advanced adversaries

In this scenario operations still take place within the home base but against a more advanced adversary. This may be an invasion from another state or civil unrest supported by an advanced opponent. The architecture takes a more hybrid approach and still uses some cell based and fixed infrastructure but supplements with more robust military communications (Figure 3). It is assumed the opponent will attempt to disrupt communications by kinetic and cyber means. The

electromagnetic spectrum will be more contended with the enemy seeking to deny its use. A well equipped opponent will target vulnerabilities in cell based communications. This could lead to information being compromised or the network being blocked preventing information flow. Military communications systems will provide better Transmission Security (TRANSEC) and flexibility. In high intensity conflict the network will have to adapt quickly as the tactical units manoeuvre to gain advantage. MANET and connections to engineered links at the strategic level will allow the network to adapt to changing circumstances and enemy action.

This architecture provides a robust and adaptable network. It will not be able to offer the throughput or low latency of a fixed infrastructure. The entire network infrastructure will be organic to the tactical units and thus additional physical security will not be required. The cost of this specialised military equipment will be greater than utilising existing or commercially available equipment. To mitigate this smaller numbers may be bought for immediate action and training with an ability to quickly increase holdings during escalation to war.

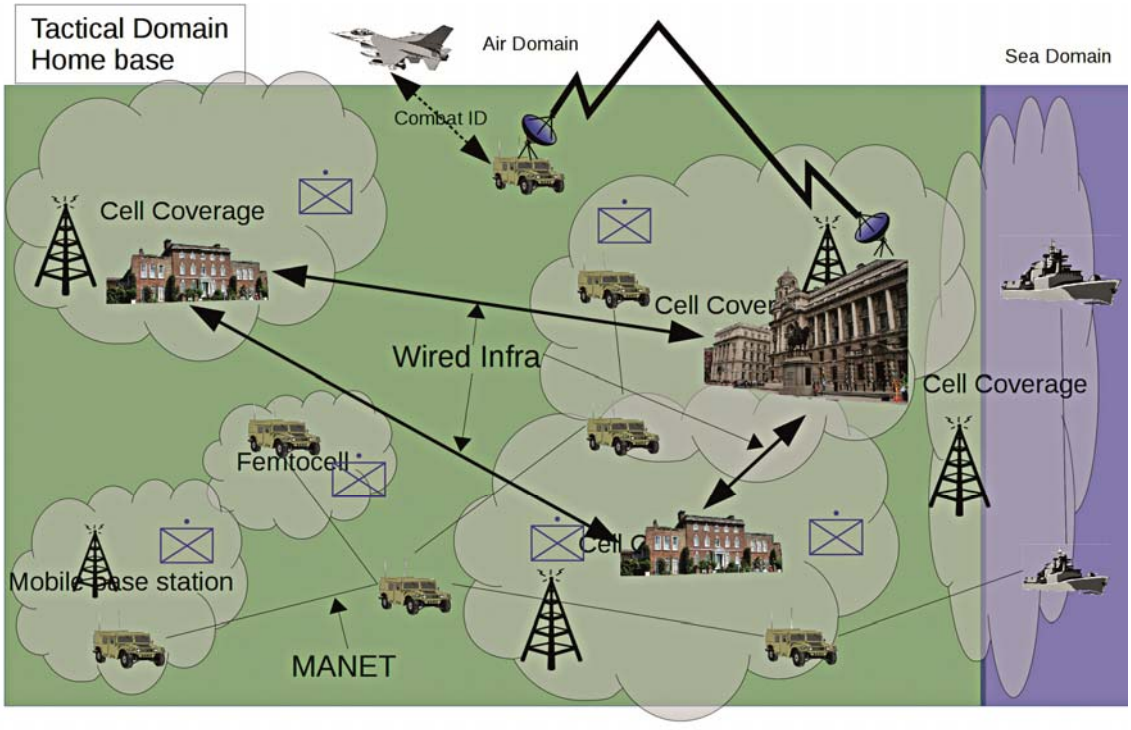


Figure 3. Protection of the home base from advanced adversaries

5.5 Military operations outside the home base – low intensity

In this scenario a country is deploying forces outside its own borders. This would be for low intensity operations such as disaster relief, humanitarian or peace enforcement. The host nation, depending on how advanced they are, could have communications infrastructure. The infrastructure could be used in a benign environment but may be compromised due to disaster, an opponent or the number of other agencies trying to utilise them. The architecture uses cell services where available but also allows military MANET where the force density and deployment allows (Figure 4). Satellite communications are used for reach back to the home base but also for disadvantaged users out with cell coverage or typical MANET distances.

The architecture for this sort of operation needs to be flexible as the situation will change. Fixed cell networks may not be accessible initially but may become available later. If many agencies or nations are in the area it will put great demands on infrastructure and spectrum availability. Whilst the generic software architecture remains the same, external connections to relief agencies or the host nation may be required. This can be established by implementing the needed formats and protocols on the ESB and connecting via a firewalled connection.

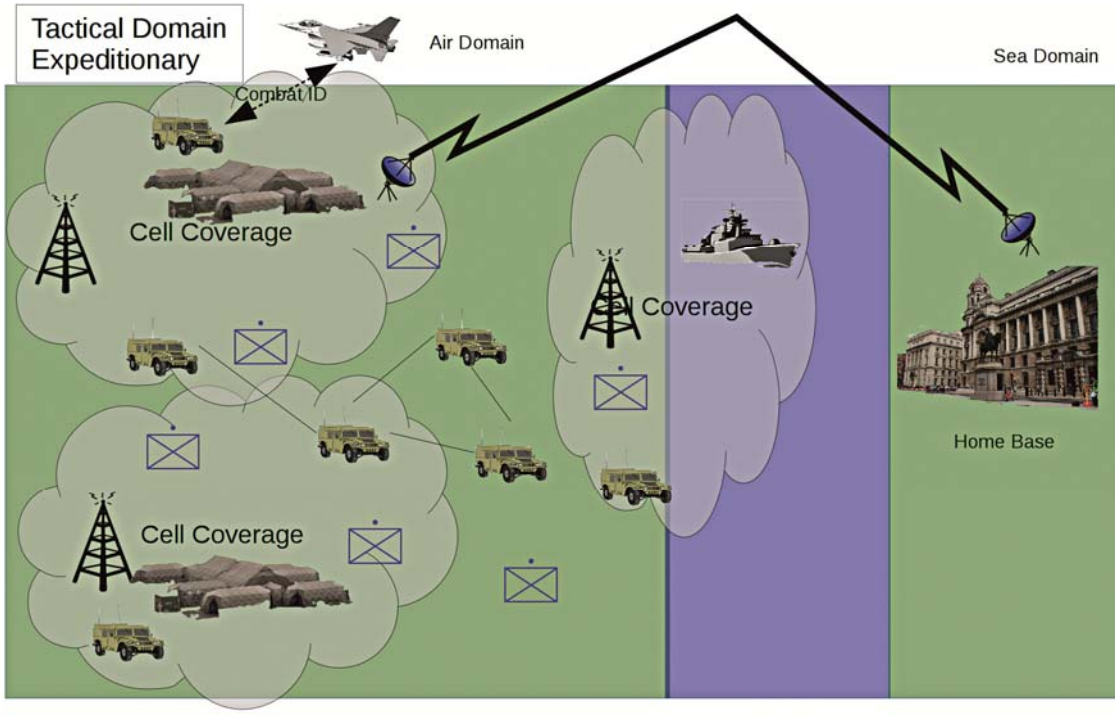


Figure 4. Military operations outside the home base – low intensity

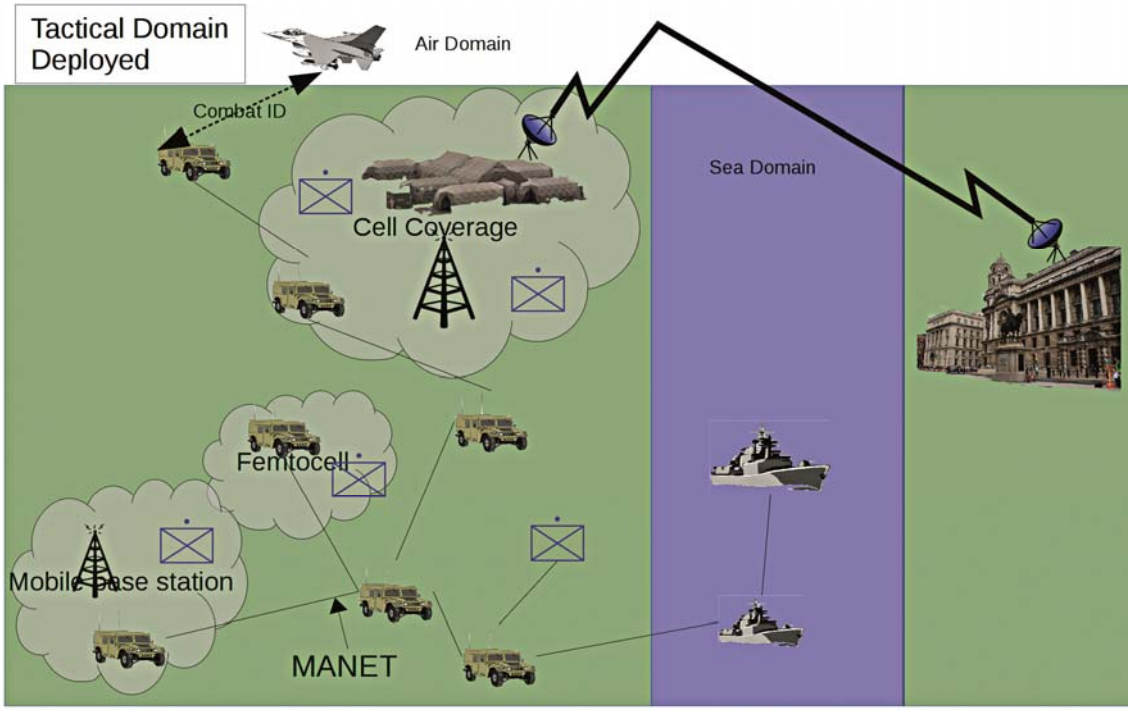


Figure 5. Military operations outside the home base – high intensity

5.6 operations outside the home base – high intensity

In this scenario a country is deploying a conventional force in to high intensity conflict in another area. This is likely to be as part of a coalition so interoperability is important. Access to any infrastructure or availability of spectrum is likely to be very limited. Enemy action and own forces manoeuvring will have a large impact upon network topologies. The enemy could be technically capable and hence the use of civilian infrastructure could have risks in terms of availability and cyber attack.

The architecture is mostly based on military off the shelf equipment but does allow a mix of cellular technology where the situation allows (Figure 5). The cell base stations could be deployed by the force as semi-permanent base stations of as mobile femtocells.

The reliance on military technologies will mean that throughput will be reduced from that provided in a more fixed infrastructure. The network should be more resilient to enemy action and to electronic warfare.

6. Other Lines of Development

The technology and the architecture presented will only become a usable system once the other lines of development are considered and developed.

Doctrine and training must allow the user to not only use but exploit the system to provide military capability. The system must be supported by a clear support strategy. Personnel must be properly trained and the lines of support documented and understood.

Transition to service can be very disruptive when new systems and ways of working are rolled out. The nature of the suggested technologies and the architectural approach lend themselves to a gradual roll out. The software architecture could be rolled out across a legacy data network. The use of the ESB can allow legacy applications to share data more easily with others on the system. This also allows benefits to be accrued early and avoid a disruptive transition.

The approach to the acquisition process must allow the same flexibility that is in the architectural approach. One vendor providing the entire solution, whilst simpler to contract, leads to vendor lock in and the pace and cost being set by that vendor. By ensuring open standards and with the use of open source technologies the right vendors can be selected for the given technologies. By favouring open source software it is also possible to change vendors mid development without losing the work already done.

This approach to acquisition requires an intelligent customer who understands the user need as well as the technology. Where possible this should come from within the military but when those skills are not available contractors separate and independent from the main suppliers should be used. It is important that the military should retain all the Intellectual Property (IP) and system ownership of the design and architecture.

7. Conclusions and future work

In this paper some of the key technology elements that could help specifying an independent tactical domain have been covered. The need for flexibility and independence from fixed solutions has been emphasised.

An architectural approach which provides a standards based network by the most efficient means for the tactical environment is proposed. The software layer has several methods to ensure flexibility as well as ease of implementation and maintenance. The use of containerisation ensures that applications are isolated and easily upgradable. The embedding of an ESB in the architecture ensures that data can be shared and structured for exploitation by semantic tools. It aids interoperability and makes the transition from legacy applications more seamless.

The technology itself is not sufficient to deliver military capability. The other elements must be considered and aligned with the technology development. An acquisition approach that retains as much IP and power within the military rather than a single selected vendor is preferred.

A number of candidate architectures were given as an example rather than a template as it is important for the commander and their J6 staff to retain flexibility. The scenarios show a range of intensities both in and out of the home base. Any operation will be unique with its own restrictions and requirements therefore the architecture will be planned based on matching the available capabilities.

Future work should look at the efficiency of the proposed technologies in a deployed tactical network. Particular emphasis should be put on a distributed architecture that avoids points of failure and makes efficient use of the underlying network.

References

Akyildiz, I.F. et al., 2008. A survey on spectrum management in cognitive radio networks. Communications Magazine, IEEE, 46(4), pp.40–48.

Ali, M., Hailong Sun & Wei Yuan, 2013. An Efficient Routing Scheme for Overlay Network of SOAP Proxies in Constrained Networks. In High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International Conference on. pp. 466–473.

Bard, J. and Kovarik Jr, V. J., 2007 Software defined radio: the software communications architecture. Vol. 6. John Wiley & Sons.

Bhattacharyya, B. & Bhattacharya, S., 2013, Emerging Fields in 4G Technology, its Applications & Beyond-An Overview. International Journal of Information and Computation Technology, Volume 3, Number 4 (2013), pp. 251-260

Carlucci, G., De Cicco, L. & Mascolo, S., 2015. HTTP over UDP: an Experimental Investigation of QUIC. In Proceedings of the 30th Annual ACM Symposium on Applied Computing. SAC '15. New York, NY, USA: ACM, pp. 609–614.

Chappell, D., 2004. Enterprise service bus, O'Reilly Media, Inc.

Clancy, T.C., Norton, M. & Lichtman, M., 2013. Security Challenges with LTE-Advanced Systems and Military Spectrum. In Military Communications Conference, MILCOM 2013 IEEE. pp. 375–381.

Dua, R., Raja, A.R. & Kakadia, D., 2014. Virtualization vs Containerization to Support PaaS. In Cloud Engineering (IC2E), 2014 IEEE International Conference on. pp. 610–614.

Goeller, L. & Tate, D., 2014. A Technical Review of Software Defined Radios: Vision, Reality, and Current Status. In Military Communications Conference (MILCOM), 2014 IEEE. pp. 1466–1470.

Ha, S.H. & Yang, J., 2013. Classification of switching intentions toward internet telephony services: a quantitative analysis. Information Technology and Management, 14(2), pp.91–104.

Hartman, A.R. et al., 2011. 4G LTE wireless solutions for DoD systems. In Military Communications Conference, MILCOM 2011. pp. 2216–2221.

Jarschel, M. et al., 2011. Modeling and performance evaluation of an OpenFlow architecture. In Teletraffic Congress (ITC), 2011 23rd International. pp. 1–7.

Johnsen, F.T. et al., 2013. Evaluation of transport protocols for web services. In Military Communications and Information Systems Conference (MCC), 2013. pp. 1–6.

Joint Capabilities Integration and Development System (JCIDS) Manual, 2012.

Johnsen, F.T. et al., 2013. Evaluation of transport protocols for web services. In Military Communications and Information Systems Conference (MCC), 2013. pp. 1–6.

McKeown, N. et al., 2008. OpenFlow: Enabling Innovation in Campus Networks. *SIGCOMM Comput. Commun. Rev.*, 38(2), pp.69–74.

Mitola, J., 1995. The software radio architecture. Communications Magazine, IEEE, 33(5), pp.26–38.

Mitola, J. & Maguire, G.Q., 1999. Cognitive radio: making software radios more personal. Personal Communications, IEEE, 6(4), pp.13–18.

NATO Interoperability Standards and Profiles, 2014, FMN Architecture, Available through: http://goo.gl/a03JIC

RFC768 - Postel, J., User Datagram Protocol, RFC 768, August 1980. (http://tools.ietf.org/html/rfc768)

RFC793 - Postel, J., Transmission Control Protocol, RFC 793, September 1981. (http://tools.ietf.org/html/rfc793)

Royer, E.M. & Chai-Keong Toh, 1999. A review of current routing protocols for ad hoc mobile wireless networks. Personal Communications, IEEE, 6(2), pp.46–55.

Saarelainen, T. & Timonen, J., 2011. Tactical management in near real-time systems. In Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2011 IEEE First International Multi-Disciplinary Conference. pp. 240–247.

Schnabel, O. & Hurni, L., 2009. Cartographic web applications–developments and trends. In Proceedings of the 24th international cartography conference, Santiago.

Singh, R.K., Joshi, R. & Singhal, M., 2013. Analysis of Security Threats and Vulnerabilities in Mobile Ad Hoc Network (MANET). International Journal of Computer Applications, 68(4).

Stewart, R. (2007), "Stream Control Transmission Protocol", RFC 4960, Internet Engineering Task Force.

Tortonesi, M. et al., 2013. Enabling the deployment of COTS applications in tactical edge networks. IEEE Communications Magazine, 51(10), pp.66–73.

Vankka, J., 2005. Digital synthesizers and transmitters for software radio, Springer-Verlag New York, 2005, 359p.

Vankka, J., 2013. Performance of Satellite Gateway over Geostationary Satellite Links. In Military Communications Conference, MILCOM 2013 IEEE. pp. 289–292.

Zimmermann, H., 1980. OSI Reference Model--The ISO Model of Architecture for Open Systems Interconnection. Communications, IEEE Transactions on, 28(4), pp.425–432.

Zoughbi, G. et al., 2011. Considerations for Service-Oriented Architecture (SOA) in military environments. In 2011 IEEE GCC Conference and Exhibition (GCC). pp. 69–70.

Enabling Circle of Trust in High Security Environment

Klaus Zaerens
Finnish National Defence University
Klaus.Zaerens@iki.fi

Abstract

Trust management has been a topic of keen interest in recent years. There has been a lot of discussion as to what new opportunities it can bring to markets, what benefits it can offer, and what system development possibilities it enables for software development. In this paper we discuss trust management in a military context. We examine the key features of the Circle of Trust in public authority environments. We address the most essential problems and obstacles to be considered before the benefits of Circle of Trust can be fully enabled therein. As a solution to problems with the information transfer management, we propose a novel approach utilizing the modern cryptographic technology. The discussion and views presented in this paper can be adopted in any organization with doubts concerning the sensitive and classified contents of current ICT systems.

Keywords

Trust management; Cryptography; Security; Military

1 Introduction

Importance of trust management is increasing as the Internet is more open for access, different collaboration tools and social networking become more common. The relevance of trust management is gradually becoming more significant, but the multilateral nature of the concept, generally trustworthy parties and large data sets with high response time requirements have kept commercial activators and applications away from production use in public authority environments.

Public authorities in security field have sought and developed numerous means to improve cooperation by ICT solutions. Different kind of collaboration tools and environments has been deployed and integrations between systems and data storages have developed. It is obvious that concepts like semantic knowledge processing, connectivity and social networking enable improved cooperation between authorities. However these concepts cause also new challenges. Openness can be hard to manage in highly secured environment. Also processing of the critical operative information increases hostile interest on system environment.

In public authority environment the trust to other stakeholder is unreserved in relation to profession and officiality. In collaboration and cooperation context, participating authorities compose virtual community with only trusted parties. We call this kind of consortium as a circle of trust. Within circle of trust, the participant

shares information in order that the other participants will improve their succession in operations. This enhances the overall performance of the virtual community from which every participant gain benefit.

The special case of information sharing is to delegate operative situational data for improving situational awareness in the circle of trust. This kind of collaboration improves the accuracy of the individual awareness in each actor and enriches the awareness of all actors within operation. This cooperation enables better communications, safe procedures and more effective actions in operations throughout participating authority organizations.

In this paper, we will discuss issues and problems to be considered when implementing circle of trust concept in core authority systems. We define the key features and characteristics of such a high security environment. We also characterize the environment's limitations and provide examples of corresponding measurable parameters. We will narrow our observations to military systems in which the need for computational capacity is high and the reliability of information is always critical. In military environment we must ensure data flow correctness. In this paper we discuss on a situation where a trusted node forfeited credibility and we should control the information or knowledge the node receives from our trusted network. As a solution to problems with the adoption of circle of trust in public authority environments, we propose an approach that manages the delivery of information within the closed circle of trust and improves the security of overall system by reducing the risk of information being compromised.

2 Situational Awareness and Trust Management in Military Context

Improving situation awareness has become more critical in public authority operations and especially in military context. The possibilities and utilizations of situation awareness have increased together with technical evolution. Sensors and mobile devices increase the effectivity of collecting data from locations that traditionally have been difficult to access. More data can be collected and stored than previously, which enables view on situation to be more truthful, accurate and comprehensive.

The most severe challenges on improving situation awareness are related to refinement of significant information from huge amount of data, unstable data transfer connections and especially in field operations, limited data capacities [1]. Also data correctness, reliability, redundancy and timeliness have been research issues or discussed in several publications [1]. Less discussion has been addressed to trust evaluation of the data source or the security issues on delegating the situational data to recipients with different trust levels. This aspect is relevant in military environment where there is always possibility for a malicious actor is receiving our confidential information or sending unreliable data to our decision making process.

In this paper we adopt the definition of trust presented by Grandison and Sloman because of the simplicity yet complete enough. Trust is "a quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context" [2]. Moreover, in this paper we limit our observation on computative trust management. Widely accepted features on computative trust management include subjectivity, the expected probability and relevance [3, 4].

In military context participants of the trust relation are bound to a role. A participant represents some actor or unit within an organization. Unit has a task and a goal and special expertise specified by the organization. It is important to understand that when two actors from different units interact, one trusts the represented role not the actor itself. Yet the trustworthiness between two roles can be fixed on process level, the individual actor might have specific preferences, interests or experience which affects to quantitative trust. Similarly, data providers such as sensors can be modelled as an actor in trust relation and represented by an ownership of an organizational unit.

3 Circle of Trust characteristics and benefits in Military environments

In this paper we define Circle of Trust as a consortium of a specified subject with only trusted parties. It means that each participant has sufficient amount of trust to other participant in relation of the subject. The sufficient can be considered as readiness for deliver and receive knowledge unconditionally without risking own operative ability. The motivation for creating the consortium is to construct a united force to gain improved capability in operations with same goal. For achieving the goal it is essential to have an open and transparent information exchange between the participants. To sustain the circle, all parties should have indirect or direct benefit from collaboration and cooperation with each other. The participants rely operative enhancement that they gain from the participation of the circle. Enhancement can be for example improvement of efficiency in operative actions or overall reduction of operative costs. In practice the actions can be trading situational information between participants. Moreover we argue that the Circle of Trust formed by combining the public authorities from different countries is the only real possibility to improve the situational awareness in order to operate successfully in cyberwar. Malicious actions in cyberwar are conducted always from international level and often routing is hiding the origins of the actor. Resolving the actor needs international collaboration with openness of information. We should not forget that defending from malicious action on national level can be only reactive by nature. That is why countermeasures are effective only when performed also on international level. The information collected by international consortium can help to identify the existence of malicious actor and to detect false information from the attacked systems.

The example of Circle of Trust is illustrated in Figure 1. In Figure 1 *A* represents us as a situational information provider. *B* and *C* are recipients of our information. Arcs represent the direction of information. Because information trading should happen in both directions, arcs are represented also from the recipient to us. Each arc contains two parameters *s* for situational information and *w* for the weighted trust between information provider and recipient. It is notable, that if for example $w_{AC} \neq w_{AB}$ then $s_{AC} \neq s_{AB}$,. In practice this means, that the situational information provided by the provider is not the same unless the trust relation between provider and recipient are exactly the same. It can also be noted that the trustworthiness of the recipient is in direct relation to the correctness and completeness of the situational information provided by the information provider.

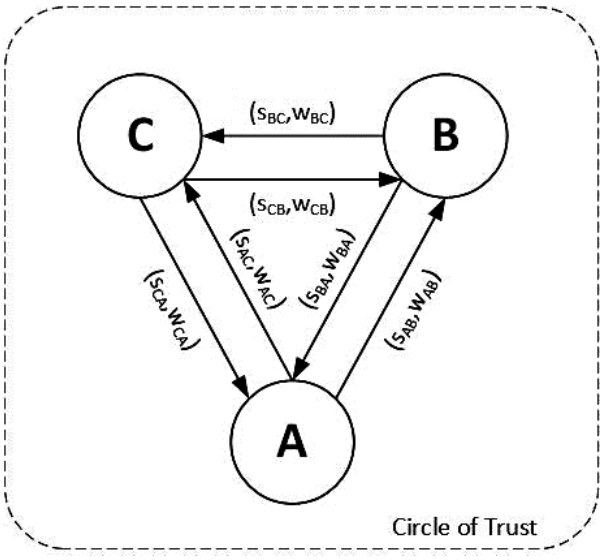


Figure 1. Circle of Trust

As stated before, with Circle of Trust situational awareness can be improved by trading the intelligence and reconnaissance information within the participants of the circle. Trading is usually mutual sharing where the quality and the amount of traded information are in balance.

The trading can also be used for identifying possible leakages. If there is a suspected malicious actor as a member in Circle of Trust, with labelled or water marked information to participants it is possible to detect and identify the source of leakage by following the trace of the information. If there is certainty of an intrusion to system, with Circle of Trust deceptive information can be fed to malicious actor without breaking the routines and not disconnecting the actor from the grid too soon. More over the capabilities of a hostile actor can be monitored and evaluated by observing the actions it performs in controlled environment.

Circle of Trust is a scalable and generic concept. In international scale we can consider a military alliance such as NATO as an example of Circle of Trust. On national scale example can found from the collaboration with public authorities of safety like between police forces and rescue service. On organizational level we can have example from ministry like Ministry of the Interior and all the agencies that it conducts. On the technological level all nodes in a high security network can form a Circle of Trust.

4 Some challenges within Circle of Trust in High Security Environment

In this chapter we discuss more on challenges identified within the Circle of Trust. The circle of trust should enable openness of information exchange, but the openness also increases the risk of revealing too much sensitive information to public.

Situation data contains always some information about the collector or origins of data by nature. This information can relate to location information, resources or capability. This information can be used against the originator. Revealing information is always risk and the delivery should be somehow controlled so that the information, knowledge or capabilities are not leaked to any hostile or untrusted recipient.

4.1 Absolute trust does not exist in reality

Within closed Circle of Trust, some parties are always more trustworthy than others. For example in military alliance some nations are in more deep cooperation than others and some nations can have doubts from history to others. In that sense the sufficient amount of trust can be varied a lot between the actors. The consequence is that the participants in the Circle of Trust are not in the same level. In authority cooperation trust within own organization is usually unreserved. This trust is based on mutual experience, common procedures and professional community. A lot harder is to trust another authority and different organization. We can find this element of distrust in each level of Circle of Trust concept. The main concern is the leakage of sensitive information illustrated in Figure 2. After revealing situational information for recipient *C,* we are not able to manage the revealed information. If *C* has a connection with party *D*, which does not belong to our original Circle of Trust, *C* might still provide some information to *D*. Assuming that *A* is the only information source, the *D* will receive information $s_{CD} \subseteq s_{AC}$.

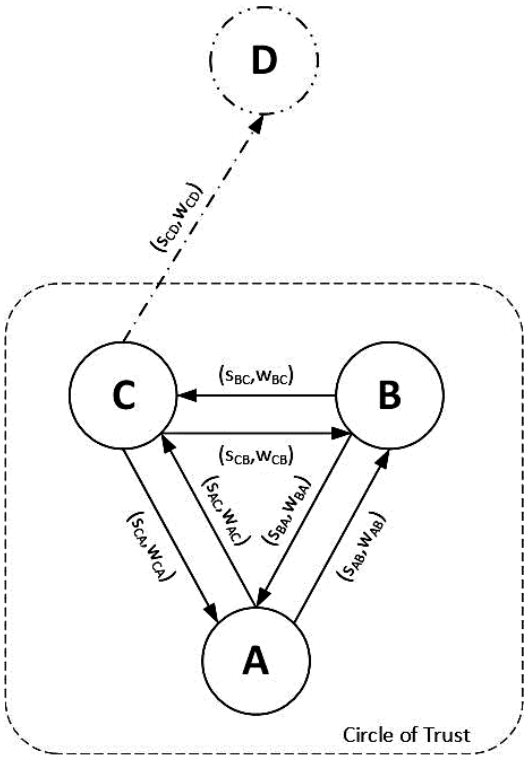


Figure 2. Leakage of situational information

Another dimension of this challenge is the publicity of distrust. If one actor is not ready to release all information unconditionally to all other actors but is bound to principality of openness within the circle, how publicly this limitation of released information can be made.

4.2 Managing information delivery in open network

In previous chapter we discussed on leakage of information. Regardless of how much we have trust on our allies, we need their information. To receive information from other parties the usual convention is to give or send information collected by the one. This actually forms a trading system where tradable information is defined by its usefulness, timeliness, trustworthiness, accuracy and comprehension. As stated in previous chapter, absolute trust does not exist in reality. Circle of Trust or any alliance is trying to form a framework where quality levels of information are agreed in written and we can rely that at least the exchange of information itself actualizes. Information providers try to minimize the amount of sent information but still receiving the maximum amount of information. The main goal of the recipient is to have sufficient amount of information to form awareness of a situation. The interesting question is that what is the sufficient amount of provided information to gain that goal?

Another issue arises when information is sent to the recipient. After transmission of information the provider loses all control to the sent information. That when a receiver has interpreted the information, the receiver immediately owns the information and can use it to any purpose needed. This includes also sending the

information to other partners, avoided or simply not intended by original source. Having secured connection does not solve this issue since for the received information is presented as decrypted form.

The accumulation of information can be also a problem. This situation is illustrated in Figure 3. If *A* sends data fragment s_{AB} to recipient *B* and data fragment s_{AC} is send to recipient *C*, it is possible that both of the recipients send the data fragments to less trustworthy participant *D*. *D* can combine the both data fragments $s_{AB} \cup s_{AC}$ and create more comprehensive situation and indirectly form an increased threat to the originator *A*.

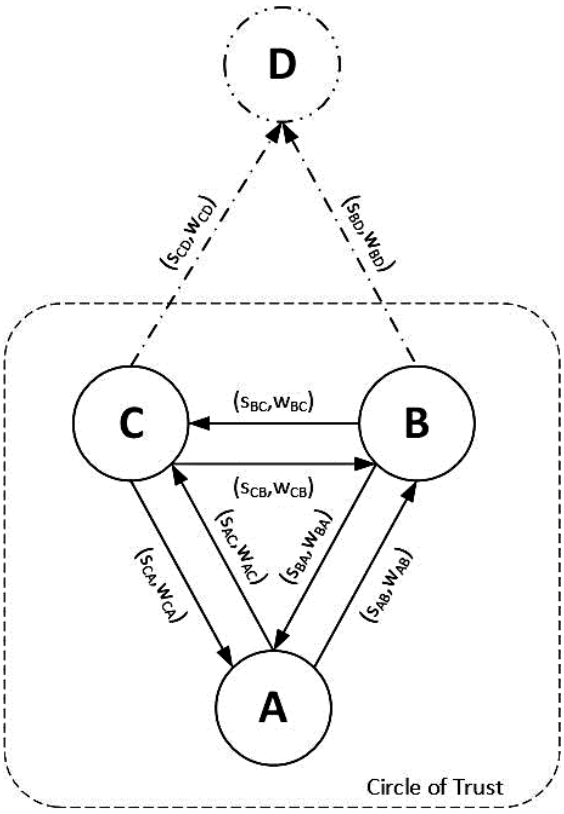


Figure 3. Accumulation of situational information.

4.3 Collateral damage of deception

Previously we described the possibility of deception with the identified intrusion in the secure environment. The challenge is how the intrusion is notified to other participants in the circle without risking that the information is reached to the intruder. This problem setting is formalized in Figure 4., in which *A* has some distrust with *C* (i.e. w_{AC} is small) and wants to send false information s_{AC}. At the same time *C* and *B* have a strong trust relation (i.e. w_{BC} and w_{CB} are great) and also *A* and *B* trust each other. If *C* transmits the information s_{AC} as s_{CB}, *B* receives false data which can be very harmful of course for *B*, but also for *A*. After exposure of deception the trustweight w_{BA} is most probable to decline, which influences the future information exchange and trade balance.

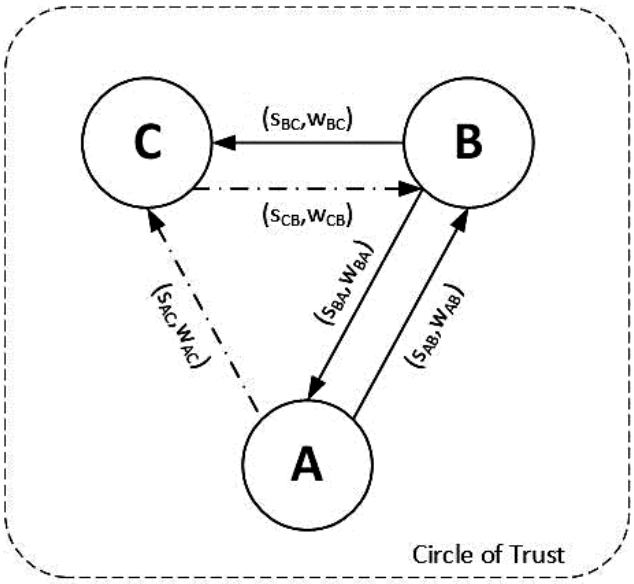


Figure 4. Collateral damage of deception.

A special case of this problem occurs when one participant in Circle of Trust identifies an intruder within the Circle. If the other participants are not trustworthy enough to identify the intruder and the deceptive data is fed to the intruder, how can we notify the other participants not to trust information that they receive from the intruder.

5 Overcoming obstacles by utilizing cryptographic technology

In this chapter we present a proposed solution to overcome problems in previous chapters. We adopt the latest research results in cryptography conducted by Huang et al. [5, 6, 7, 8]. Huang presents a novel approach to existing public key encryption schemes. For our problem we utilize his commutative encryption algorithm based on ElGamal encryption [6, 9]. With commutative encryption we are able to encrypt information more than once with different public keys. The usefulness in our problem is that the decryption order may vary as needed.

In our approach the basic idea is to reveal all the possible solutions of situation awareness for each counterpart. The participants have individual keys for encryption of the solution, but they are not aware the accuracy or exact trustworthiness of the decrypted information. In principle everyone has access to every decrypted solution, but only the source, the provider has the information of correct original information and which key has the best decryption in order to have original information. The approach is illustrated in Figure 5. $f(A_{key})$ is the encryption on original information provided by A which results the encrypted information A'. For each recipient there is a key which decrypts the information with f' resulting the recipient specific information (in Figure 5 [*B, C, D*]). It is noteworthy that there should be a key or several keys for parties outside the Circle of Trust.

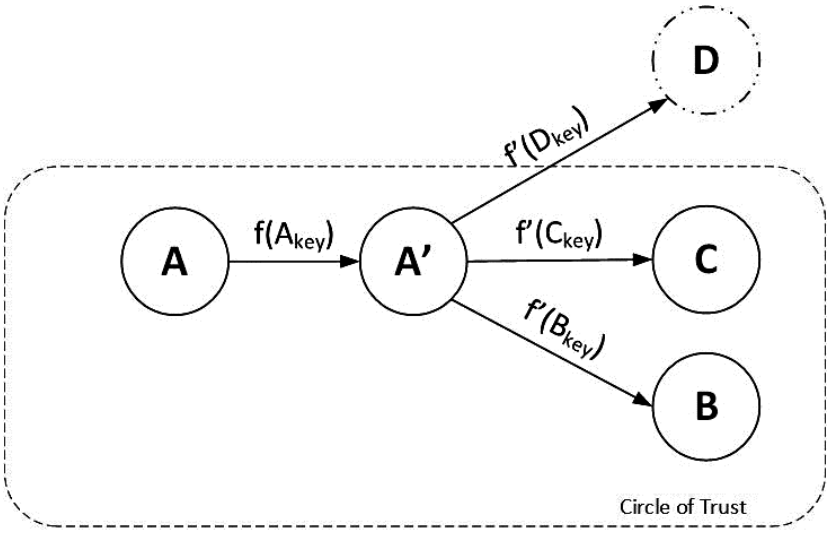


Figure 5. Encryption and decryption of information with different levels of trust.

In practice this is achieved by encrypting the information so, that the each of the decryption key results a valid outcome. According the Huang encryption $f(A_{key})$ contains all the encryption for each recipient. That is $f(B_{key})$, $f(C_{key})$ and $f(D_{key})$. After keys are delivered to recipients the encrypted information is opened for open access. Solution relies on the fact that none of the recipients knows the actual trustworthiness of their received decryption. For example with information trading between B and C the differences can be identified, but the accurate reliability cannot be solved. In Table 1 the example of information modification is presented. Here the modification is made on observation level, but it can also be on object attribute level. Trust level represents how much trust we have on the recipient and how accurate information we want to provide.

Table 1. Example of information modification towards partners with different trust levels.

	Own correct information	**Open Public Information**	**Decrypted with key *B***	**Decrypted with key *C***	**Decrypted with key *D***
Trust level	100	0	90	50	10
Observation 1	A red car	Vehicle	A red car	A car	A blue car
Observation 2	A fighter plane	Aerial vehicle	A plane	A plane	UFO
Observation 3	An assault helicopter	Aerial vehicle	An assault helicopter	A helicopter	Vehicle
Observation 4	Drone	Aerial vehicle	Drone	UAV	UFO

For a computational issue, the malicious actor has no possibility to decrypt all possible solutions and if they do that, they are not aware which one of the results is the most accurate representation of the encrypted information. Moreover we argue that even if the malicious actor could collect all the decrypted instances of the information from certain time, it cannot reliably determine what represent the best information. For example in Table 1 recipient *D* might have a problem resolving is the observation 3 a land vehicle of an aerial vehicle. Also outsider cannot solve what kind of aerial vehicle observation 4 is.

We are aware that this solution works best in timely systems where the amount of information is huge. Of course with infrequent high security information exchange other conventional encryption methods are more useful.

It should be also noted that in Circle of Trust all participants are not necessarily directly bound to each other. All participants within the Circle are bound to each other at least with transitive trust. Despite the unconditional trust exists within the whole circle of trust, the absolute trust is decreased depending the amount of transitions and their relative trustweights. This construction forces to control the delivery of information in order to prevent the leakage of information and knowledge.

At the end we want to emphasize that presented approach is scalable from different abstraction levels of Circle of Trust. It applies to multinational organizations as well as high security network information exchange between nodes.

6 Related work

In this chapter we will present a brief overview of existing concepts and technologies that are discussed similar problems such as Circle of Trust. First we observe the Knot concept.

Circle of Trust can be considered as a virtual community. That sense it is shares the similar context than Gal-Oz et al. have presented in their approach on knots [10]. A knot is defined as a subset of community members identified as having overall strong trust relations among them by directly from trust model of indirectly via transitive trust. Moreover knots are groups of members that can rely on each other's recommendations even if they did not rate the same experts. However the Gal-Oz model emphasizes the symmetry of trust. In Circle of Trust, trust might vary also when changing the recipient to a sender and vice versa. It means that the trust between the actors is not symmetrical. In some cases recipient has to rely the information provided by the provider, even if there is a suspicion that the information received is not good quality. Despite the doubt, it might be that the information traded back is best that can be provided. This kind of asymmetric situation occurs when the trading parts have significantly different capabilities of providing and testing the reliability of transmitted data. The technically stronger and with larger resources can use deception at some extend and demand full accuracy and highest quality in return. In other words, trust varies between the actors in the context of Circle of Truth. The Knot concept should contain also a mechanism for weighed trust relations. In that way we can quantify the distrust in Circle of Trust.

Second we examine the idea of trust transitivity. Jøsang et al. have published several papers where they have discussed on features and possibilities of trust transitivity [11]. This research has a potential platform for enhancement where transitivity is limited by threshold when weighed arcs are chained. However this does not avoid the fact that the first recipient owns the received data after interpretation. Trust

transitivity method needs an external broker to control the threshold of the chained arcs. We still find that kind of system vulnerable for exposure of data.

Third we point out that Chen et al. [12] have published a methodology where attributes of trust are delegated subjective trust evaluation. The approach should consider the aspects of distrust and include some mechanism to avoid exposure of data regardless of the trust values. However, delegation of attributes and building a global trust map can quantify the accumulation problem and at least increase the knowledge on leaked and possibly accumulated information. It might also be interesting approach by itself to the collateral damage of deception problem, because the trust values can prevent sending distrusted information via trusted arcs.

7 Conclusions

In this paper we examined the Circle of Trust concept within the military context. We stated that the absolute trust never exists and information exchange is necessary in order to build a comprehensive situational awareness. We identified the three primary obstacles to adopting Circle of Trust in a military context and examined possible solutions to overcoming them. We proposed a new approach by using modern cryptographic technology. We ensure the secrecy of own collected sensitive data by releasing different versions of information for different recipients. This is done by encrypting the information simultaneously with different keys which are delivered one for each recipient. The decryption result can be controlled on encryption phase. We argue, that revealing all solutions of decryption is so large, any malicious actor has no capability to solve in reasonable time which solution has most accurate information in which parameter.

References

[1] Zaerens, K, Enabling the Benefits of Cloud Computing in a Military Context, Proceedings of 2011 IEEE Asia-Pacific Services Computing Conference (APSCC'11).

[2] Grandison, T, Sloman, M, Specifying and analysing trust for internet applications, In Proceedings of the Second IFIP Conference on e-Commerce, e-Business and e-Government, 2002.

[3] Abdul-Rahman, A, Hailes, S, A distributed trust model, In Proceedings of the 1997 New Security Paradigms Workshop, pp.48-60, 1998.

[4] Zhou, Z. X., Xu, H, Wang, S.P, A Novel Weighted Trust Model based on Cloud, Advances in Information Sciences and Service Sciences, 2011.

[5] Huang, K, Tso, R, Chen, Y, Rahman, M, Almogren, A and Alamri A, PKE-AET: Public Key Encryption with Authorized Equality Test, The Computer Journal first published online April 20, 2015 doi:10.1093/comjnl/bxv025

[6] Huang, K, Tso, R, A commutative encryption scheme based on ElGamal encryption, In Information Security and Intelligence Control (ISIC), 2012 International Conference on IEEE, 2012, p. 156-159.

[7] Huang, K, Tso, R, Chen, Y. C, Li, W, Sun, H. M, A New Public Key Encryption with Equality Test, In Network and System Security, Springer International Publishing, pp. 550-557.

[8] Huang, K, Chen, Y. C, Tso, R, Semantic Secure Public Key Encryption with Filtered Equality Test - PKE-FET, SECRYPT 2015, p. 327-334.

[9] El Gamal T,. A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, 31(4), 1985, p. 469-472.

[10] Gal-Oz, N, Gudes, E, Hendler, D, A robust and knot-aware trust-based reputation model, Proceedings of the 2nd Joint iTrust and PST Conferences on Privacy, Trust Management and Security (IFIPTM 2008), Trondheim, Norway, pp. 167–182, 2008.

[11] Jøsang, A, Pope, S, Semantic Constraints for Trust Transitivity, Proceedings of the 2nd Asia-Pacific conference on Conceptual modelling-Volume 43. Australian Computer Society, Inc., 2005.

[12] Chen, B, Zeng, G.S, Li, L, Attribute Delegation Authorization Based on Subjective Trust Evaluation, 2008 IFIP International Conference on Network and Parallel Computing, 2008.

Authors

Jouko Vankka is a professor in the Department of Military Technology in the Finnish National Defence University (NDU) since 2012. He received the M.S. and Ph.D. degrees in electrical engineering from Helsinki University of Technology in 1991 and 2000, respectively. He received the Degree of Bachelor of Social Sciences from Helsinki University in 1994. Since 2005 he has been with the Finnish Defence Forces.

Heidi Krohns-Välimäki was born in Joensuu, Finland, June 1985. She received her M.Sc. from the Department of Electrical Energy Engineering, Tampere University of Technology, Tampere, Finland, in March 2010. Since April 2010 she has been a researcher in the Department of Electrical Engineering at TUT. Her research interests include situation awareness in major disturbances of the electricity supply.

Jussi Haapanen was born in Kirchheim unter Teck, Germany in 1990. He received his M.Sc. in 2015 from the Department of Electrical Engineering, Tampere University of Technology. Since 2015 he has been working as a researcher at Tampere University of Technology. His research interests include information systems for managing disturbances of electricity and telecommunication networks.

Niina Nissinen is an engineer officer in the concepts and doctrine division at Finnish Defence Research Agency in Riihimaki, Finland. She received her M.Sc. degree from Helsinki University of Technology in 2009 and is currently a Ph.D. student at the National Defence University. She works as a researcher at the FDRA in the operations analysis team.

Klaus Zaerens is a PhD candidate at the Department of Military Technology in National Defence University Finland. He received his MSc from the Department of Computer Science, Helsinki University in 2008. He has defined and managed deliveries of customized large capacity information systems in the field of telecommunications, finance, traffic and public sector from the year 1999. His research interests include cloud computing, distributed systems and transaction management in a high security environment.

Stuart Marsden spent 16 years in the British Army leaving at the rank of major in 2012. He had a varied career which started in logistics, transitioned to information technology and then tactical communications. Since leaving the military he has consulted for defence firms internationally and begun studying for a PhD in Military Technology at the Finnish National Defence University.

National Defence University
P.O. BOX 7, FI-00861 HELSINKI

Tel. +358 299 800

www.mpkk.fi

ISBN 978-951-25-2720-5 (nid.)
ISBN 978-951-25-2721-2 (PDF)
ISSN 2343-2357 (nid.)
ISSN 2343-2365 (PDF)

Puolustusvoimat
The Finnish Defence Forces