FFI-rapport 2014/00187

Integration of chemical and radiological sensors in a tactical network

John Aasulf Tørnes and Erlend Larsen

FFI Forsvarets forskningsinstitutt

Integration of chemical and radiological sensors in a tactical network

John Aasulf Tørnes and Erlend Larsen

Norwegian Defence Research Establishment (FFI)

1 September 2014

FFI-rapport 2014/00187

1238

P: ISBN 978-82-464-2422-4
E: ISBN 978-82-464-2423-1

Keywords

CBRN-stridsmidler

Deteksjon

Nettverk

Approved by

Berit Harstad Gilljam	Project Manager
Janet Martha Blatny	Director

English summary

The Chemical and Radiological (CR) sensors in the Norwegian Armed Forces today are stand-alone units giving alarms locally to the personnel in close proximity to the sensor. Other troops are alerted through the chain of command, but the information may be unnecessarily delayed or distorted. Networking the sensors will enable rapid and consistent dissemination of warnings to other units operating in the same area. In addition, if responses from several sensors are fused and sent to a decision support tool, it is easier to discover false alarms and give recommendations with a higher degree of confidence.

This report describes how CR sensors could be connected and the information fused in order to obtain a better operational picture of CR events which may take place. A simple detection algorithm is proposed to fuse information from several identical personal chemical sensors. The fusion of information from sensors using different detection principles will provide more accurate information than using sensors with only one detection principle. One use case is where information from multiple sensors could be pushed into a geographical information system (GIS), to allow the leader of a search-team to get an overview of the search area in near real-time.

Different sensor networks could be used for different purposes. Personal CR sensors require less communication resources, whereas specialized instruments require higher transmission capacity and possibly dedicated communication resources to an off-site laboratory for expert assistance.

Existing communication networks are recommended for sensor communication, as long as the sensors are either fitted on soldiers or mounted on vehicles. On the other hand, if sensors are to be placed at a distance from existing radios, they will have to be equipped with their own means of communication.

It is recommended that a computerized system to store and handle the raw data or consolidated data should be installed in order to be able to retrieve the data at a later stage. It is also important to take networking into account when procuring new sensor systems. For some of the existing sensors, new communication modules need to be purchased.

Sammendrag

De kjemiske og radiologiske (CR) sensorene i det norske forsvaret i dag er frittstående enheter som kun gir alarm til personell i nærheten av sensoren. Andre enheter varsles gjennom kommandokjeden, men man risikerer at informasjonen blir unødig forsinket eller endret. Sammenknytting av sensorer i nettverk vil gjøre det mulig raskt å sende ut varsel til andre enheter som opererer i det samme området. Dersom man kan se responsen fra flere sensorer sammen og sende resultatene til et beslutningsstøtteverktøy, er det lettere å oppdage falske alarmer. Det vil i tillegg være mulig å gi anbefalinger med større grad av sikkerhet basert på sensorresponsen.

Denne rapporten beskriver hvordan CR-sensorer kan sammenkoples i et nettverk for å gi en bedre situasjonsforståelse etter at CR-trusselstoffer er brukt. En enkel deteksjonsalgoritme er foreslått i denne rapporten for å sammensmelte informasjonen fra flere personlige kjemiske sensorer av samme type. Sammensmelting av informasjon fra sensorer med ulike deteksjonsprinsipp gir mer informasjon enn sammensmelting av informasjon fra like sensorer. Et brukseksempel er overføring av sensorinformasjon fra flere sensorer inn til et GIS-verktøy, slik at lagføreren i et søkelag vil være i stand til å få oversikt over søkeområdet i nær sann tid.

Det vil være behov for ulike sensornettverk for ulike formål. Personlige sensorer krever færre kommunikasjonsressurser, mens spesialistinstrumenter krever høyere overføringskapasitet og muligens dedikerte nettverk tilbake til eksperter ved et eksternt laboratorium.

Eksisterende kommunikasjonsnettverk kan benyttes for kommunikasjon mellom CR-sensorer så lenge de enten bæres av soldatene eller er montert på kjøretøy. Dersom sensorene isteden skal plasseres på avstand fra eksisterende radioer trenger de egne kommunikasjonsmidler.

Det bør installeres et datasystem for å lagre og håndtere rådata eller sammenslåtte data slik at disse kan søkes opp i ettertid. Det er også viktig å planlegge for at sensorene skal kunne monteres i nettverk ved anskaffelse av nye sensorsystemer. For noen av de eksisterende sensorene vil det være ønskelig å anskaffe kommunikasjonsmoduler.

Contents

Preface

This report has been written as a collaboration between the Cyber Systems and Electronic Warfare Division and the Protection and Societal Security Division at the Norwegian Defence Research Establishment (FFI). This collaboration has been initiated to take advantage of several different areas of expertise within FFI motivated by the network centric warfare paradigm within the Norwegian Defence.

1 Introduction

Defence against chemical, biological, radiological and nuclear (CBRN) warfare agents is an important function within the Norwegian Armed Forces. Today, most of the chemical and radiological sensors (CR sensors) are stand-alone instruments where the generated information is accessible only to the soldier or unit carrying the sensor. Other troops rely on receiving the information through the command line, with the risk of untrained or missing personnel delaying or distorting the information. In addition, the information from only one sensor may give an inaccurate understanding of the situation, e.g., through a false detection or the missing ability to map sensor detections geographically. Merging the information from several sensors may improve the information quality significantly, such as in Figure 1.1, where the distance and direction to a gas release may give valuable information for force protection and threat neutralization.

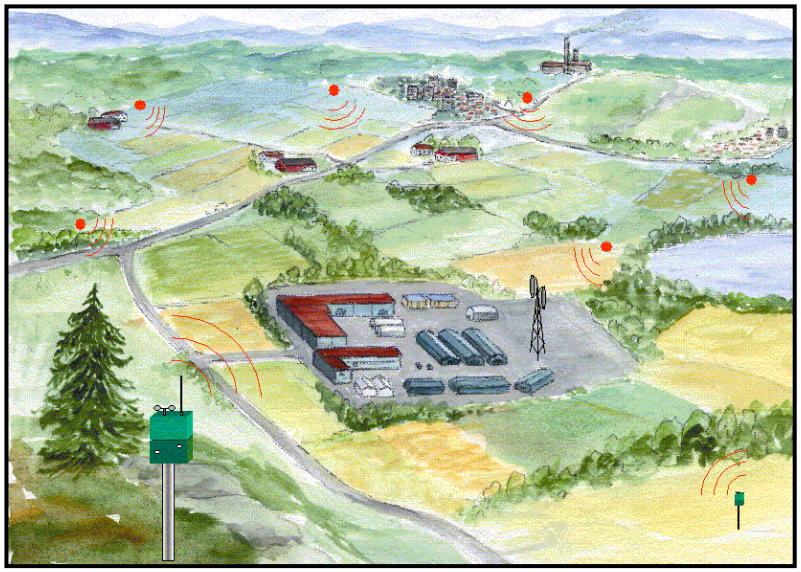

Figure 1.1 Networked sensors around a military installation. (Illustration: FFI).

Net-Centric Warfare (NCW) has high priority in the Norwegian Defence Long Term Plan 2011-2012 [1]. In the NCW concept, capacities and actors are networked together using information technology. The networks in NCW consist of people, and the networking takes place between the people in these networks. The information flow is not necessarily defined by the hierarchic military command structure, and the aim is to utilize all available resources efficiently, obtaining a more complete basis for decision. The motivation behind NCW is to increase the speed of the OODA-loop[1], to make better decisions faster than the enemy.

The introduction of NCW will increase the information load on the soldiers, and it is important to reduce unnecessary work load. Thus, the specialist soldiers should not be burdened with easily automated tasks. Routine tasks increase the probability of lack of

[1] Observe, Orient, Decide, Act (OODA)-loop. A decision-cycle concept often applied to the combat operations process. See S. Diesen, “Manøverkrigføring i det 21. århundre: Er mekaniserte styrkers storhetstid forbi? [25]

attention, which can eventually lead to mistakes and errors. One such routine task is the manual copying of information from CR sensors from one platform to another. This could for example be information from personal or vehicle-mounted sensors to a CBRN decision support tool. Today, this is done by using voice messages to pass sensor readings to a local headquarters (HQ) (e.g. company HQ), where it has to be typed into a mail-system before it is sent to a higher level (battalion or brigade HQ). Instead, this could be done using an automatic data transfer. It is recommended that the soldiers use limited time and resources on interpreting the information from CR sensors and on comparing them to information from other sources. The CR-sensor information could automatically be sent up to the next level in the chain of command if not stopped by the local CBRN officer or unit commander. The ability to stop the message locally is important, to reduce the number of false alarms transferred to higher commands. It is most often local forces that have the best situational awareness (SA) of what is going on in their area and are the best personnel to classify the alarm as true or false.

It should be emphasized that while networking CR sensors may allow for quicker dissemination and improved SA, a man in the loop will always be needed in order to interpret and validate the fused CR sensor information. However, CBRN defence specialists will always be a limited resource in the military organization. Automation of tasks not requiring human evaluation may therefore be vital to allow better use of the scarce human CBRN resources in order to improve the SA and response.

During the last years, and especially since the events that took place on July 22, 2011, there has been increased focus on civilian – military cooperation and how their resources could be better utilized if such a tragedy happens again. In order to get the best possible use of both military and civilian CR detection resources, they should be able to share sensor information, preferably on similar platforms using the same software. It would be beneficial if CR sensor information from the military and civilian side could be fused[2] together to obtain a better operational picture. Today there is no such sharing of sensor information.

The work described in this report is an attempt to summarize the concept on how chemical and radiological sensors could be networked in the Norwegian Armed Forces as a part of the work that Norwegian Defence Research Establishment (FFI) carries out in the FFI-project 1238 (*CBRN-vern*) to support the procurements in the Defence Project P9511 (Detection, Warning and Reporting). It is focused on the need for data networks and data fusion on a tactical level. The need for data networks that operate on a strategic level is not dealt with here.

[2] Data fusion is a multi-level process dealing with the association, correlation, combination of data and information from single and multiple sources to achieve refined position, identify estimates and complete and timely assessment of situations, threats and their significance (Joint Directors of Laboratories).

The work is focused on the networking possibilities in the Army and Navy, but could also be used for the Home Guard and the non-flying personnel in the Air Force. Biological detection is not part of the FFI-project 1238 and is therefore not discussed in this report. The ideas are, however, equally important for chemical, biological and radiological sensors. In the EU project TWOBIAS (Two Stage Rapid Biological Surveillance and Alarm System for Airborne Threats), the aim was to develop a reliable biological surveillance and alarm system.

Chapter 2 of this report describes information management from networks of sensors within the Norwegian Armed Forces and Chapter 3 addresses sensor data storing. Chapter 4 describes various types of networks, while network communication is dealt with in Chapter 5. Discussion and further work is given in Chapter 6, and Chapter 7 concludes the report.

2 Information management

Modern military or civilian units might carry several CR sensors. The sensors may either use the same detection principle or different detection principles. If they use the same detection principle, they could dismiss one alarm as false if none of the other sensors have responded. If they use different detection principles, they could detect CR agents that cannot be detected by one sensor alone.

In order to give the operator the best possible SA, the sensors should work together. In that respect, it is essential that the sensors are able to transfer information to other sensors or decision-makers in one way or another. It does not necessarily mean that the information should be sent out to a wide area. This depends on the situation; the information could be shared only within one squad, or it could be sent out to a much larger area, depending on the situation or on the unit having the sensor.

In order to establish an efficient network of sensors[3], the CR important sensor data, the data recipients and the sensor fusion algorithms must be selected.

2.1 Sensor network

A sensor network consists of spatially distributed autonomous sensors to monitor physical or environmental conditions and to cooperatively pass their data through the network to the recipients. A network of sensors may be transformed into a sensor network through implementing local processing. If all CR relevant raw data from all deployed CR sensors should be passed to the HQ unprocessed, the HQ personnel would be overloaded with information and would not be able to extract the important and correct parts of the data. In addition to the transmission of data, some means to fuse the information from different sensors should therefore be included, to indicate which sensors are supporting one decision

[3] There is a difference between the terms “sensor network” and “network of sensors”. The first term imply intrinsic interactions between the sensors and is therefore “smarter” than a network of sensors where no such interactions takes place.

and which sensors are in opposition to this decision. The network of sensors will thereby become a sensor network.

A sensor network could consist of sensors with the same detection principle or with a combination of different principles. If several sensors provide an alarm, it is possible to determine the extent of the contaminated area. If only one sensor in a network gives an alarm, the detection might be classified as false if not verified by other means. It is better, however, to have sensors using different detection technologies (sometimes called orthogonal sensors). If two or more orthogonal sensors give consistent alarms, the detection could be treated with a higher degree of certainty. The Lightweight Chemical Detector (LCD) and the Chemical Agent Monitor (CAM), both from Smiths Detection, use the same detection principle (Ion Mobility Spectrometry, IMS) and are therefore not orthogonal sensors. LCD and AP2C or AP4C from Proengin are on the other hand using two different detection principles (IMS and flame photometry) and could therefore be considered orthogonal.

In a recent report on the FFI-project "Situational Awareness Sensor Systems (SASS)", wireless sensor networks (not CR sensors) have been described and technologies to communicate and retrieve data from sensors have been proposed. This was tested during field trials at Rena Military Camp and at Kjeller during September 2012 [2]. However, these sensor networks were designed to be immobile, with sensors that could lie unguarded. CR sensors today are cost demanding and large in size, and are also difficult to hide from the enemy or from civilian groups if left without guarding. The CR sensors will therefore more realistically be personal or placed on vehicles on land or vessels at sea. Networking these sensors and fuse the information from them to obtain the best possible operational picture could give operational benefits.

2.2 Which sensor data should be transmitted through the network of sensors

The amount of information that is available from a sensor depends on the type and complexity of the sensor. Only a small amount of data is available from for example a LCD. From the LCD model 3.1B, only the detected agent types, G (nerve agent) or H (blister agent), is shown on the sensor display. From the data-port on the sensor it is also possible to read out the relative concentration level (one to eight bars) and an indication of the type of chemical warfare agent (CWA) detected to an external device (Figure 2.1). From a more advanced sensor, for example a portable mass spectrometer, much more data is available, making a higher level of identification (tentative or provisional) possible.

Figure 2.1 A Lightweight Chemical Detector (LCD) showing a nerve agent alarm (right) connected to a radio (left) and a personal data assistant (middle) (Photo: FFI).

From non-specialist sensors, it will normally be necessary to send sensor data (raw data or treated data) only upwards through the chain of command. These sensors produce only small amounts of data (a few bytes), and they could normally not be remotely programmed via a network. The sensor data will be collected and treated at some point in the chain of command. This data treatment could be a comparison of data from several equal or different sensors, and also a comparison with information from other sources, e.g. intelligence data. The consolidated data might then be sent downwards back to lower units as orders or information messages. This is already in place as text messages (e.g. as XO-mail or link-16 messages) within the military.

Generally, it will be necessary to send more data (mega- or gigabytes) upwards from detection instruments used by specialist forces. The specialists might need to pass raw data back to a reachback laboratory (e.g. FFI) for assistance in interpreting the data. Special software packages might be necessary on both sides, and the data transmission might need higher capacity compared to what is necessary for information from personal sensors.

2.3 Some software packages in use today

For CR-sensor information, and even for other sensor types, better and more easy-to-understand information could be sent by using map-based decision support systems. Such systems, e.g., Maria from Teleplan and CBRN-Analysis from Bruhn NewTech, exist within the Norwegian Armed Forces, but are not in common use for presentation of CR-sensor information in Norway.

CBRN-Analysis from Bruhn NewTech is a computerized CBRN hazard prediction, intelligence decision support and warning and reporting tool. It is mainly designed to provide

military commanders with rapid and accurate information using real time reports from source level to higher commands. The program automates the CBRN calculations laid down in NATO's Warning and Reporting publications, ATP-45 [3] and AEP-45 [4] and is currently in operational use in over 90 % of NATO and Partnership for Peace (PfP) nations [5].

Bruhn NewTech also provides a Sensor Connectivity Information Management tool (SCIM), which is a software hub that provides sensor connectivity to multiple sensor types and brands in a single display [5]. It filters the data from sensors and instruments and allows that information to be transmitted for further analysis. SCIM only collects, filters and displays separate data sets and does not carry out any sensor data fusion.

Maria 2012 Geo Development kit from Teleplan Globe AS is a collection of building blocks that can be used by a developer to assemble a tailored Geographical Information System (GIS) application [6]. It contains a set of independent modules that enables rapid development of highly tailored GIS applications.

The SAAB Automatic Warning and Reporting System (AWR) is designed to provide early warnings to units and personnel in CR danger on the battlefield. In Sweden, the soldiers do not possess personal CR-sensors, but have their sensors mounted on vehicles or in the field. The AWR system consists of nodes, i.e. alarm units and sensor nodes, which could be meteorological, chemical, biological, radiological, positioning, video etc. (www.saabgroup.com) [7]. One AWR mobile platform unit can connect up to eight sensors from different companies, mounted in a dedicated box (see Figure 2.2).

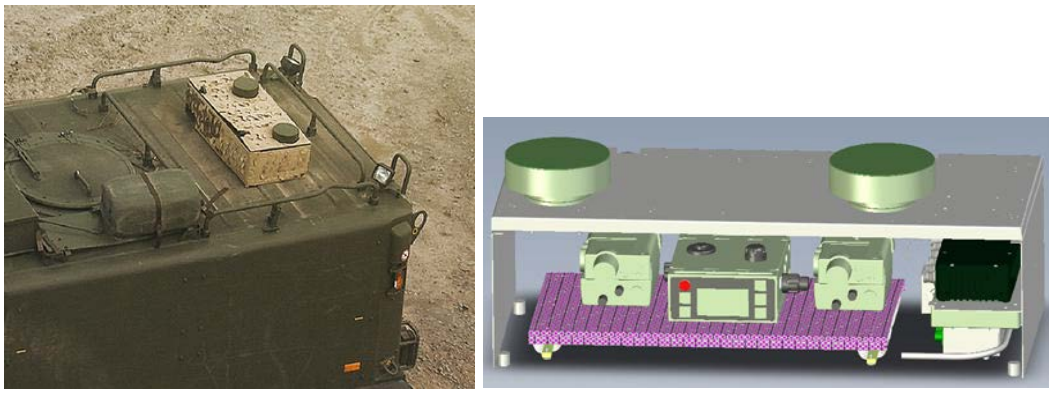

Figure 2.2 Automatic Warning and Reporting System (AWR) mobile platform from SAAB mounted on the roof of a vehicle (left). The box could contain up to eight different chemical and radiological sensors (right) [8].

The sensor box is connected with a single cable to the mother vehicle, where CR-sensor information will be passed to CR experts at a higher level in the chain of command (Figure 2.3). According to the information from SAAB, they are working on sensor fusion to increase the reliability and to reduce the false alarm rate. It is not clear how far they have come in this work [8].

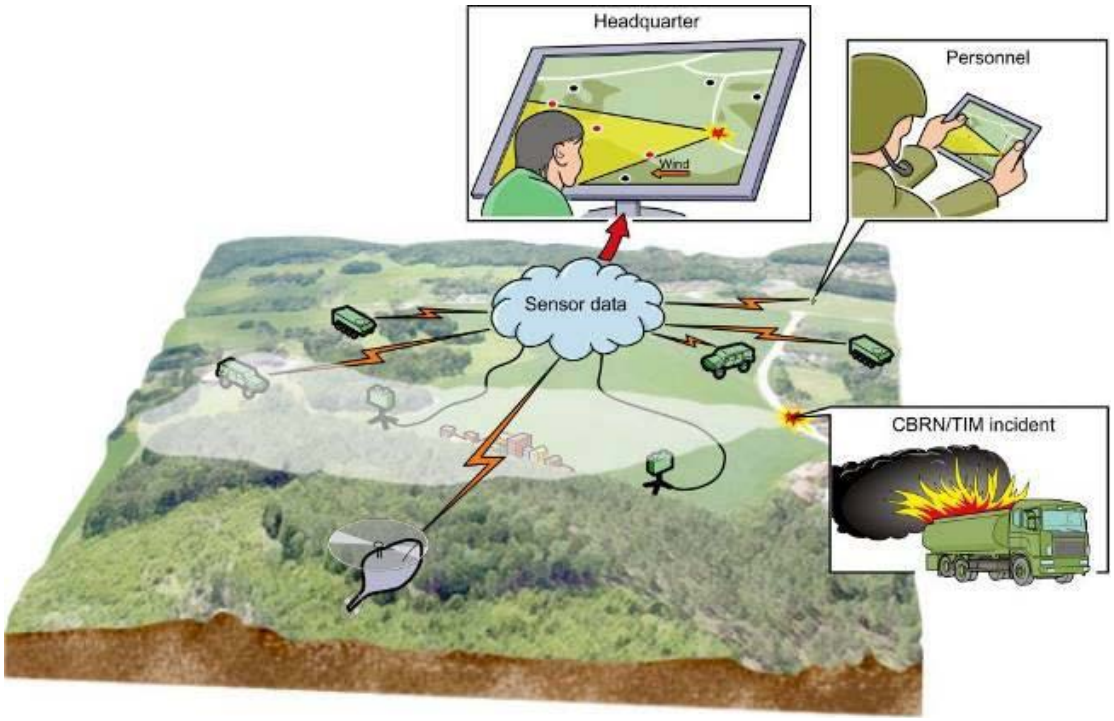

Figure 2.3 The SAAB Automatic Warning and Reporting System (AWR) [7].

2.4 Data fusion

It has to be decided where in the chain of command the raw data from sensors should be collected and treated (fused). It is the view of the authors that this data fusion should be done at a low level in the chain of command, where first-hand information on possible CR incident exists. Troops on the site will also be the best personnel to judge whether the alarm is false or true, based on what the sensors have been exposed to.

Sometimes the personnel at the site have limited education and training in interpreting alarms from CR sensors. In such cases it is important to be able to quickly transfer the alarm message to experts at a higher level without having to re-type the message into another program. The experts may then give quick assistance back to the exposed unit.

Based on these assumptions, the data from non-specialist sensors could be fused at squadron level in the Army, Home Guard and Air Force or at each ship in the Navy. Fused and validated data could then be sent up through the chain of command. At some point the validated data should be imported into CBRN decision support systems like CBRN-Analysis or Maria. These software packages require expertise to use and will not be available at low level.

Data from instruments used by CR defense specialists do not need to be fused at a low level. This could for example be data from the mass spectrometer in the Fuchs Search and Surveillance Vehicle (from Rheinmetal) or data from gamma spectrometers. Some of these data are raw data that the specialists need in order to interpret the results. It is also important

for the specialist to be able to send data back to a reachback laboratory for assistance in the data interpretation. Raw data should be stored locally in order to be used as evidence for the discovery of CR agents.

3 Storage of sensor data

Data from detected CR agents should be stored for a defined time after alarms for exposure assessments. If people contract an illness at a later time, it is important to know, among other things, which CR agents they have been exposed to and, if possible, the quantities, and at what time the exposure took place. This is done today for the data collected by personal radiation dosimeters. This information might be needed in court if someone experiences health effects that possibly could be contributed to radiation or chemical exposure. It is therefore important to know the quality of the data. Some information of the sensor fusion process therefore needs to be stored as well, e.g., how many positive and negative sensor alarms the fused data are based on.

Stored and anonymized data could also be used in education of new personnel, as experiences from real detection of CR agents are valuable education sources.

4 Network of sensors

It is especially advantageous to connect personal CR sensors together. Such sensors are small and relatively cheap and every platoon could therefore afford to have several sensors. When networked, these sensors could together reduce the false alarm rate compared to stand-alone sensors and provide better SA for the unit. A network of sensors will also make it possible to give quicker warnings to other units operating in the same operational area.

Another use of networked radiological or chemical sensors could be to define the boundaries of a possible contaminated area. When the soldiers in a search team find a contaminated area, the results (measured activity or type and concentration of CWA) could be sent to the team leader in real time. As the search process progresses, the results could automatically be displayed in a map-engine and the team leader would be able to get an overview of the search area in near real time. When the search is finished, the finalized hazard area could then be exported to the central Command, Control and Information (CCI) system with a simple keystroke.

4.1 Which type of sensors should be networked

4.1.1 Existing sensors

Within the Norwegian Armed Forces today, there are some sensors that easily could be networked and others that are difficult to network. This is described in an earlier report [9]. The personal chemical detectors could easily be networked by purchasing new

communication and power units. This will make it possible to connect the detectors directly for example to the Normans CCI soldier system. This is both easy to do and will give the soldiers a large advantage, compared to stand-alone sensors as described in Chapter 2 in this report. The ship-mounted detectors for chemical warfare agents in the Royal Norwegian Navy are already connected to a computer network in each ship. The users could read out data from the sensor on terminals connected to this network. Today, data fusion from several sensors is not supported. Neither is data transfer to the tactical network, nor any communication between the ship-mounted CR sensors and external sensors. The Coast Guard vessels have the same type of ship-mounted sensors, but they use less classified networks compared to the Royal Norwegian Navy, which means that the information more easily could be distributed off the ship.

The connection of the small handheld radiation sensors to a network is not so straight-forward, but could be done by using a split-cable between the sensor and its detection probe or by special probe adapters designed for connecting the gamma probe directly to the network.

It is also easy to connect some versions of the Toxic Industrial Chemical (TIC) sensors from Dräger to a network. Unfortunately, most of the older Multiwarn II sensors could not be networked. The newer models (the different X-am versions) could be connected to a computer or a computer network [10].

The connection of LCD, Automess probe adapter and Multiwarn II into one integrated unit was demonstrated at FFI during the Chemical, Atomic and Toxic compound Surveillance System (CATSS) project [11-13]. Software to be able to read the data from the sensor was developed, but no algorithms for data fusion were made (Figure 4.1).

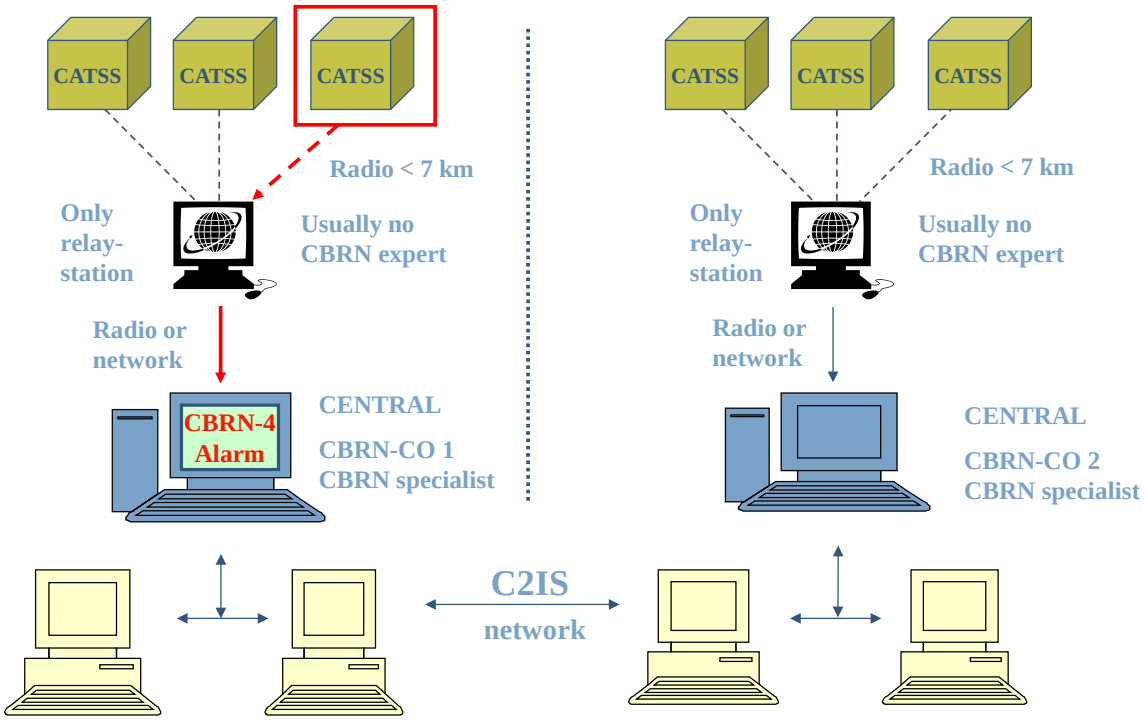

Figure 4.1 Connection of Chemical, Atomic and Toxic compound Surveillance System (CATSS) sensor units into a command, control and information network. (Illustration: FFI).

4.1.2 Future sensors

In the future, it would be advantageous to have orthogonal sensors connected in the network. Orthogonal sensors may provide reduced false alarm rates and are regarded to be a part of future developments within a CR network system. Examples of sensors which are orthogonal to the IMS-based LCD detectors are the flame photometric detectors AP2C and AP4C from Proengin or infrared spectrometers (e.g. Gasmet FTIR). During the incident at the Oslo Food Court (*Mathallen*) [14], the use of different types of sensors was found vital in identifying the threat agent.

The simultaneous use of sensors with different limits of detection and different response times will make it more challenging to define good data fusion algorithms to handle possible alarms. In such cases, one of the sensor types will alarm quicker than the other. The user will then have to decide if any actions should be made based on this first alarm alone, or if one should wait for a confirmation by the other sensor type(s).

It is important to give high priority to health and safety of the troops. Therefore, the necessary protective actions should be taken on the first indication, without waiting for a confirmation from a second sensor, unless the first alarm is obviously wrong. The implemented data fusion algorithms and messages sent out from the exposed unit will be used to warn neighbouring units, and to report the incident to higher commands. This distribution should not delay immediate protective actions.

Another example is standoff detectors that are normally placed in a secure site and scan part of the surroundings (up to a few kilometres) for the presence of chemical warfare agents (CWA) or toxic industrial chemicals (TIC). This is a way to discover toxic chemicals drifting towards the camp or the personnel, without having to deploy a search teams. In order to obtain a three-dimensional picture of the incoming gas cloud, at least two such standoff detectors need to be operating together. The information from these sensors has to be fused to obtain the needed information for the users to be able to take protective measures. A field exercise with standoff detectors was carried out in Umeå, Sweden in September 2013, and some observations are reported in [15].

4.2 What should the network of sensors look like

The structure and geographic distribution of the network of sensors depends on the operational scenario and the availability of sensors. It is only possible to give some general guidelines here, using the Army as an example.

It will not be possible to make any data fusion from one single sensor. In order to obtain any improvement, two or more sensors in each squad are necessary. The same is valid for vehicles, where one needs either two or more sensors on each vehicle, or two or more vehicles operating close together. We will therefore assume that at least two operational sensors are used within each unit.

The next question to be addressed is how large area should be alarmed immediately after confirmation by the squad leader. In our initial discussions, we have suggested that the most natural level would be to alarm the whole battalion (Bn). The Bn is one organizational unit which it is natural to alarm together. This does not necessarily mean that all soldiers within the Bn should put on their protective gear immediately. This will depend on the situation and the geographical position of the troops within the Bn.

The warning send out to the Bn could be either as a CBRN message according to ATP-45 or as plain text using the normal military message format. At the present time, using CBRN messages according to ATP-45 is too advanced for the non-specialist soldiers in Norway and will lead to more questions and misunderstandings than using plain text. We therefore suggest sending the fused message as plain text.

Immediately after a CBRN event has been observed, this should therefore be reported to the unit command post by the fastest possible means. The message should as a minimum contain [16]:

- **Date Time Group** (DTG)
- **From** (Identification of sender)
- **To** (Receiver)

- **What** has happened (i.e. type of alarm, number of bars, observed delivery method, etc.)
- **Where** has it happened (accurate description of site, map reference)
- **When** did the incident happen (DTG)
- **How** did the incident happen (more detailed description, e.g. weather data)
- **Signature** (if this is a written message)

There are several means available to send such messages. It should preferably be done in a written form to prevent misunderstandings. It could be done by using the XO-mail system already in place in the Norwegian Armed Forces, but it is also possible to use unclassified systems, like mobile phone apps. If the sensors in a unit are connected to a hand terminal, like the Normans CCI, it would be easy to send the alarm up through the chain of command without having to retype the message at several points. It is, however, important that the selected network solution is of a type which could easily be implemented also on other platforms than the Normans CCI.

4.2.1 Detection algorithm for LCDs used in the Army

FFI has made a quite simple detection algorithm that could be used to network several LCDs to Normans CCI terminals within a squad and send fused messages up through the chain of command. The algorithm is made to reduce the false-alarm rate and to increase the amount of information and therefore the SA of the members in unit. The generated message will automatically be sent upwards if not stopped by the squad leader. He/she could stop the message if it is caused by something which is obviously not related to a CBRN event, or if the sensor for example was used to take measurements of a specific object (like a barrel) under complete control of the unit. The soldier receiving the alarm will take protective measures (e.g. take on protective mask) according to their standard operating procedures, independently of the algorithms shown here. However, the algorithms will make it easier for other soldiers to get the best possible information in the given situation.

A flow diagram of the detection algorithm is shown in Figure 4.2. When an alarm is generated from the LCD, the intensity may be from one up to eight bars. A single sensor response showing one or two bars from one sensor alone can be regarded as false alarm and will not be sent to the squad leader. If, however, this low alarm (1-2 bars) is repeated from the same sensor within 60 seconds, a local alarm to the squad leader is sent automatically. The same will happen immediately, if the alarm has 3 or more bars one single time.

If the squad leader receives alarms from two or more different sensors within 60 seconds, the system will automatically transmit a global alarm up to the next level in the chain of command, if not stopped by the squad leader. The squad leader will have 10 seconds to stop the alarm before it is sent upwards automatically.

This algorithm, including waiting times, is still under test and evaluation, and could easily be changed at a later stage. This will be described in more detail in a later report.

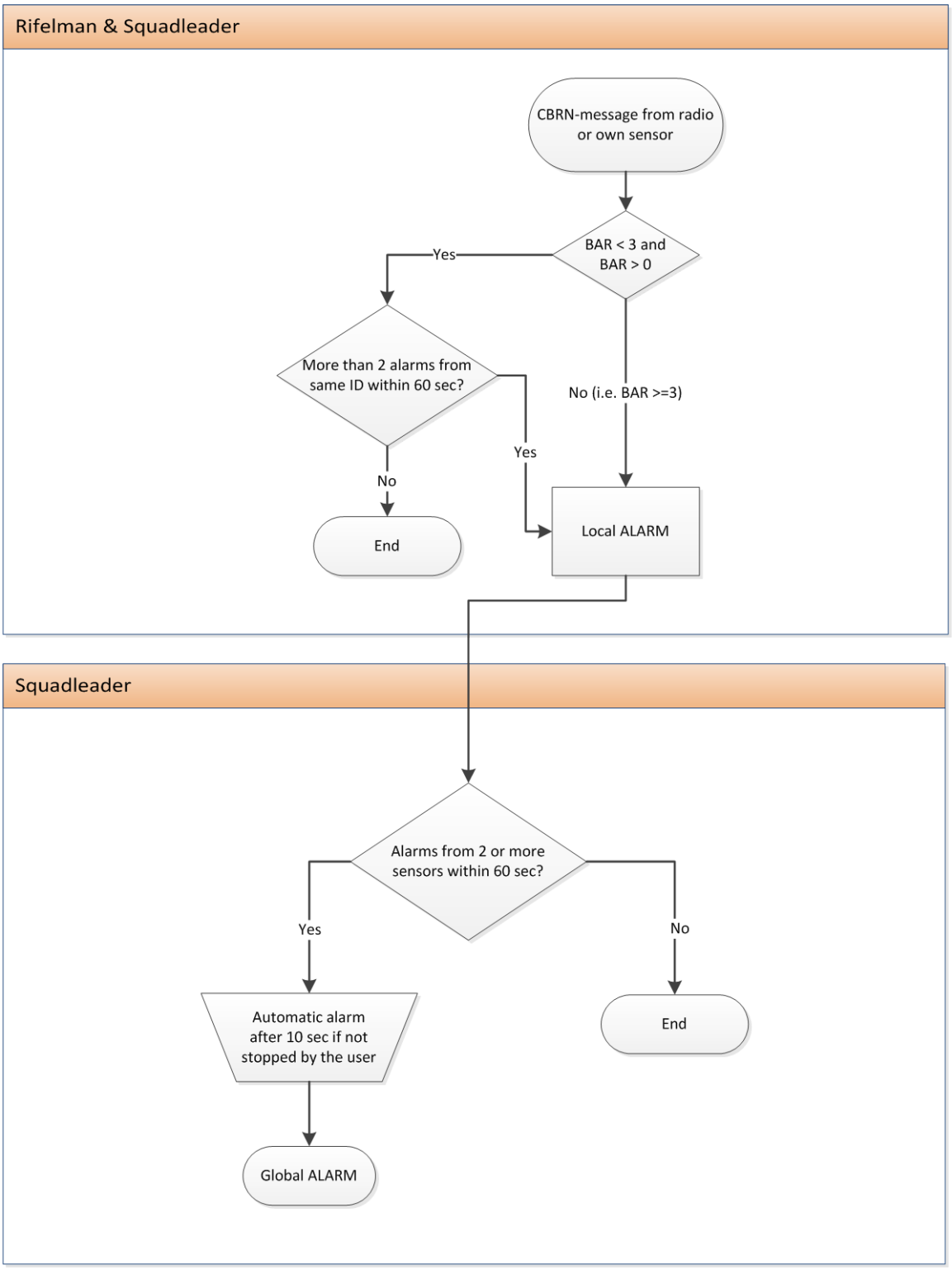

Figure 4.2 Alarm algorithm suggested for the Lightweight Chemical Detector LCD. (Illustration: FFI).

4.2.2 Network of Navy and Coast-Guard sensors

On the Norwegian naval ships, there are ship-mounted detectors for gamma radiation and for chemical warfare agents. These sensors are connected to a central computer and they are able

to show alarms directly on a computer screen. There has not been made any attempt to do any data fusion of the alarms from the sensors. The sensors are therefore acting as stand-alone units. In the ship classes with more than one chemical or radiological sensor, it is possible to implement some data fusion algorithms to handle alarms in the same manner as for the LCD detectors described above. Since some of the sensors on board ships are placed outside on deck, while others are placed inside, the signals might be difficult to compare and the advantage of data fusion might not be so pronounced as for the Army- or Home Guard-based sensors.

Landing parties from the Navy or Coast Guard will have to communicate with the mother ship through radio systems. In such operations, it will be important to be able to fuse CR sensor data and to transmit them back to the ship. The reasons for this are the same as for non-specialist sensors within the Army, and the same algorithms as described in Chapter 4.2.1 could be used for both purposes.

5 Network communication

In this chapter, we will discuss the options for networking CR sensors from a network perspective. First we will address the properties of CR sensors, and second the networking alternatives are presented, with current and future possibilities. Third, and last, the options and consequences are discussed.

5.1 Properties of CR sensors

As presented in Chapter 2, current CR sensors can be split in two groups: non-specialist, and specialist sensors. The properties of these are discussed separately.

5.1.1 Non-specialist sensors

The non-specialist sensors, such as the LCD and Automess, are cheap enough to be equipped to multiple soldiers in a platoon. Networking these sensors will give increased SA, since the aggregated information can give a geographical understanding of the CR threat, both for location and intensity.

The non-specialist sensors offer a limited amount of data per sensor, as low as a few bytes per detection. The number of sensors, on the other hand, could be as high as one per every two soldiers. The transmission rate is expected to be low in normal situations, with data transmissions limited to management information, such as alive-messages and routing. However, when a CR event occurs, all detecting sensors will generate data to be transmitted. The data can be considered time-critical. The combat-level importance of the detection will be reduced with time, so information needs to be propagated with little latency through the network. Thus, a lot of data must be transmitted in a small timeframe, without much possibility of delaying traffic to reduce the data load peaks.

The sensor traffic may be important, but at the same time it consists of much redundant information, since several sensors have made a similar detection. Data aggregation and data fusion are methods to reduce the required network resources. For traffic reduction purposes, these methods work best on converging traffic flows, i.e. flows that have a common network end point. Whether the data packets from these non-specialist sensors have a common network end point or not, depends on the further intended use of the information.

Information from the sensors may be aggregated in a central point higher up in the information structure, for instance at Bn HQ, and then pushed down to the platoons and squads again, incorporated in the Battlefield Management System (BMS). The sensor information could alternatively be accessed and processed distributedly, where local BMSs aggregate and generate a local view based on locally exchanged information. Distributed information exchange will not allow for the same degree of data aggregation and data fusion, since the information from each sensor must reach a large number of destinations in the network. Distributed information exchange will thus demand more network resources, but at the benefit of less delay between the event and the aggregated view of the event.

The security classification of the data is not determined, but if it is to be treated as classified, mechanisms to support possible encryption must be addressed. Classification may also limit the possibilities of data fusion and the placement of sensors. In addition, the sensors will be mobile, either carried by soldiers or on vehicles. This requires more effort on part of the network to establish and maintain routes from the sensors to the destination(s).

The position of sensors and their communication equipment will affect the range and quality of the data communication. As the sensors are to be placed onto vehicles or soldiers, the placement should be sought optimized for communication purposes. The number of other sensors nodes within communication range influences both the shared capacity and the possibility to reach a destination.

The available energy is an important dimensioning factor for sensor data communication. The communication range, capacity and data fusion abilities depend on the energy available, and if some sensor nodes deplete their energy storage, they are unable to forward sensor information from other sensors.

5.1.2 Specialist sensors

The specialist sensors will be fewer than the non-specialist sensors, but generate much more data. The specialist sensors will probably be placed in special vehicles, such as the Fuchs vehicle where a CBRN specialist will be located, enabling high level analysis on-site. These vehicles may also work as hubs or sinks for a subgroup of the non-specialist sensors, collecting and processing the data, along with its own measurements to generate an improved situational understanding.

Specialist sensors that are placed on a vehicle will not be limited with respect to energy, as they have access to the vehicle's energy resources.

5.2 Networking alternatives

There are two possible ways to network CR sensors as part of the operative forces today. Either the sensors are equipped with a radio interface of their own, creating a stand-alone network, or the sensor-data are communicated using existing radio systems.

A new research field, Wireless Sensor Networks (WSNs), has emerged with the development of microelectronics and wireless technology. The development has led to cheaper and more energy efficient sensor systems, based on multi-hop network technology inspired by packet routing in the Internet. WSNs are considered to be a variant of *ad hoc* networks, meaning that the network nodes are able to relay traffic for each other, to extend the range of the network. Such technology enables redundancy and automatic error correction. Through cooperation, the sensor nodes can also be capable of improving detection, and avoid or limit false alarms. The limited size and low costs facilitate systems with a large number of nodes, which are easily deployable.

A sensor node equipped with communication means consists commonly of the following components and technological solutions, both physical (hardware) and logical (software). The latter three components may be additions to existing sensors only to enable networking:

- Sensors and AD converter
- Energy source (battery)
- GPS or other means to provide position
- Processor and storage capacity
- Network interface (radio)
- Routing logic

Sensor networks are established through sensor nodes interconnecting using their radio interface and discovering routes towards a destination. A very well-known sensor network radio is the IEEE 802.15.4 [17], commonly known as ZigBee [18]. This radio has a range limited to 10 – 100 meters [19], depending on antenna elevation and obstructions. The work in [19] shows that even reducing the communication frequency does not extend the range significantly, since it is the antenna elevation that is the primary factor for limited range. The radio supports bitrates of 20, 40, 100 and 250 kbps. However, the payload bitrate capacity available per node is considerably lower. The headers at the physical and link layers take up capacity. In addition, the medium has to be accessed in an orderly fashion, while supporting the distributed network organization. In 802.15.4 this is done using Carrier Sense Multiple Access / Collision Avoidance (CSMA-CA) with random access, where the channel access is as follows:

1. Any node with traffic to send draws a random countdown time from a predetermined window. With the default parameter settings, the window spans from 0 to 2.56 ms at the 250 kbps rate.
2. The node then listens for current transmissions on the channel, and counts down to zero while the channel is free. If another node starts transmitting, the countdown is halted for the duration of the transmission.
3. Finally, the node only transmits its data when the countdown has reached zero and the channel is available.
4. Afterwards, the node waits for an acknowledgement frame. If this is not received, the packet is not considered received, and the packet is retransmitted after a new countdown time.

Thus, while the data is transmitted at 250 kbps, a lot of the time is spent waiting. Furthermore, collisions will reduce the usage of the channel further, and routing packets will also have to be transmitted. The advertised 250 kbps communication rate will not be dedicated for sensor data.

Several routing protocols for sensor networks have been developed and studied [20], to optimize critical communication parameters, e.g., the network lifetime, packet loss, and response time.

The information flow from a stand-alone network must go via gateways into the existing infrastructure. Typically, one or multiple sinks (central data destination nodes) collect data from the sensor network, and then deliver the data to a processing unit. The processed output may afterwards be pushed into a BMS, and be delivered as alarms or other information back to the end users.

There is also an alternative to creating a stand-alone network. Considering the fact that most or all nodes will be close to existing communication equipment, the sensor nodes could transmit their data through the same network that is used to transmit other SA information. One would then avoid having to equip all sensors with their own network interfaces and GPS, adding to the already high carry weight of the soldier or vehicle.

Factors that speak for employing a stand-alone network:

- The network is easily managed, as it is less complex.
- The network resources are dedicated to sensor information.
- Incorporating a sensor data exchange service as part of, or side by side with, an existing BMS is complex.

Factors that speak against employing a stand-alone network:

- Lack of range (10-100 m, unless the antennas are elevated). Using a common sensor network radio, such as the IEEE 802.15.4, will make the network vulnerable for partitioning, i.e., the radios are not able to form a connected graph where all nodes are in connection with the sensor data receiver.
- The weight of carrying another radio interface.
- The sensor network will be another network which has to handle routing and other management functions.
- The introduction of another network, which can create interference with existing radio systems.
- Data is first pushed through the sensor network for processing, outside of the existing network hierarchy, and then sent back down through a BMS. Thus, the soldiers' BMS terminals are unable to receive sensor information before it has been received and processed longer up in the hierarchy, and pushed down again.

5.2.1 Existing infrastructure, the current situation

All branches of the military service could use networked CR sensors. The Army, Air Force and Home Guard need to have SA to protect its brigade, while the Navy and Coast Guard have a need to control the environment aboard a ship, as well as protect its landing crew and landing area, e.g., during Maritime Interdiction Operations. The Army and the Navy have greatly differing communication infrastructures, but both branches are challenged with radio systems developed for defined tasks, where, for instance, IP-level interoperability is non-existent.

Figure 5.1 shows the radio networks used at the tactical level in the Norwegian Army today. The radio networks currently do not allow for data communication across the hierarchic structure. There are gaps in the lines of communication between the lowest levels and the military HQ because of both non-cooperating radio systems and security reasons. The traditional Combat Net Radio (CNR) networks are designed to operate as stand-alone isolated networks. The protocols used at the different network layers are typically non-standard protocols tuned for the specific CNR. In order for a unit to participate in the CNR network, it must be equipped with identical CNRs and radio parameters as the other units. Thus, special gateway nodes exist on boundaries between the radio networks, to allow the BMS information to be pushed upwards towards the Battalion and Brigade HQs.

There are different needs for classification of data at different levels within the hierarchy. If the data only needs to be sent upwards, the security problem might be overcome by using one-way diodes to higher classified systems. This would for example be the case for data from personal sensors like the LCD or Automess. However, allowing sensors to network horizontally, or allowing a specialist to collect sensor data while located at a low level in the radio network hierarchy, may not be possible using a diode solution.

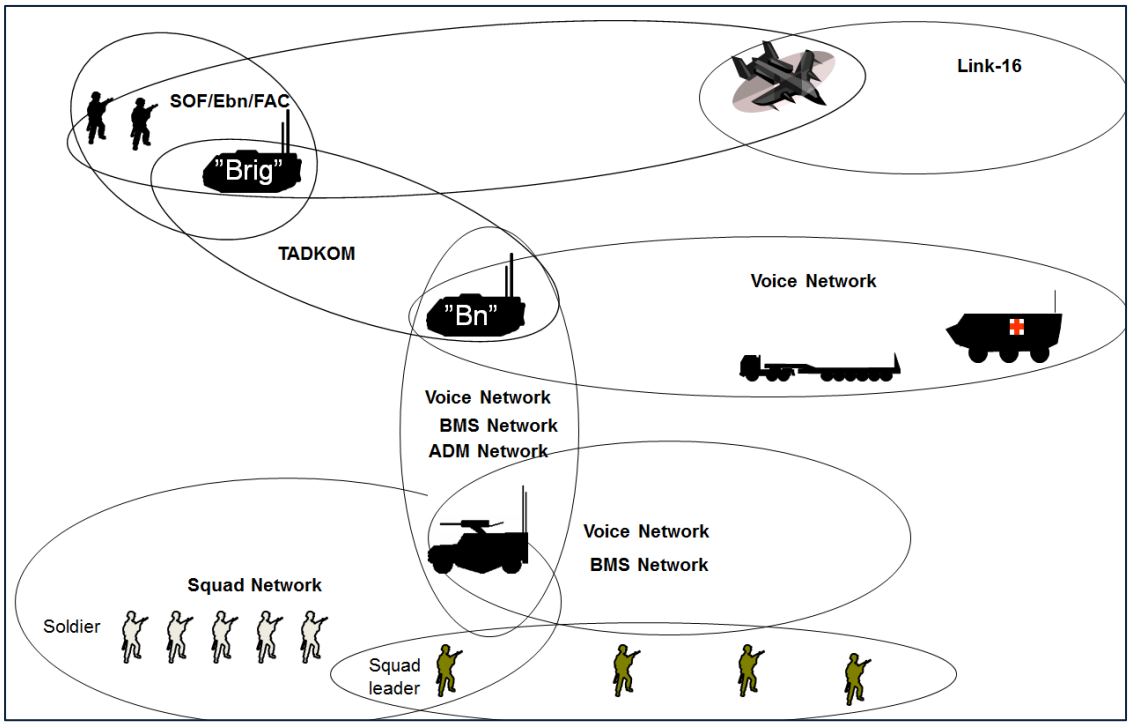

Figure 5.1 The current communication infrastructure spanning the squad to brigade level in the Norwegian Army. (Illustration: Norwegian Cyber Defence Force).

The Navy vessels are equipped with communication systems strictly specific to the task at hand, i.e., tactical data link systems (Link-11, Link-16 and Link-22), and SatCom-based operational networks for FIS Basis H and similar systems. These link systems do not directly support the transport of IP packets. NATO specifies a minimum requirement list for communications and information systems for NATO vessels in MC 195 (NATO Restricted) [21]. Existing systems can be used to network sensors by employing a tactical data link message type that is not currently in use by the connected terminals to transmit sensor data. The terminals would have to be configured to treat the message according to its new meaning. There is also a possibility to define a new national message type. However, this is not recommendable, due to interoperability problems with other nations.

Sensors may also be networked through the operations network, where IP transport is supported, but contrary to the tactical networks, the operations network may be unavailable for relatively long periods. This can be due to SatCom-shadow in fjords or a blocking mast aboard the ship. The task of the operations network is to support the operation (a timeframe of +24 hours), and not tactical maneuvers. This choice is therefore not recommended for CR sensors.

5.2.2 Existing infrastructure, future possibilities

There are several on-going defense projects to upgrade the communication infrastructure, some of which will impact and potentially improve the situation with respect to networking CR sensors:

- *P8031 Improved solutions for joint operations (Forbedrede samhandlingsløsninger)*
- *P8040 Information gateway (Informasjonsgateway)*
- *P8041 Optimization of stationary maritime radio resources (Optimalisering av stasjonære maritime radioressurser)*
- *P8043 Tactical information management system for the ground domain (Taktisk ledelsessystem for landdomenet)*
- *P8151 Interoperable SCA radios with broadband capacity (Interoperable SCA-radioer med bredbåndskapasitet)*
- *P8152 SATCOM-terminals with corresponding solutions for mobile units (SATCOM-terminaler med tilhørende løsninger for mobile enheter)*
- *P8159 Further procurement of mobile SatCom terminals (Videre anskaffelser av mobile satelitterminaler)*
- *P9217 The Defense's tactical communication nodes (Forsvarets taktiske kommunikasjonsnoder)*
- *P9271 Optimization of the Defense's communication infrastructure (Optimalisering av Forsvarets kommunikasjonsinfrastruktur)*

To support these projects, and to investigate other communication aspects, FFI have several projects on improving the military communication infrastructure, and several reports have been written on this subject. Some of this work is worth mentioning here.

FFI has been working on Network Centric Operations for many years and has described and tested a flexible Internet Protocol (IP)-network for tactical use, organized for the last years as a project program on communication infrastructure (*KI-prosjektprogram*), enveloping FFI-projects 1141 (SASS), 1175, 1249 and 1295, as well as multiple shorter assignments (*oppdrag*). The main goal is to obtain an IP-network that could be used to transport all required end-user services anywhere and on any underlying infrastructure (e.g. optical fiber, cable, and different wireless technologies). The current wireless infrastructure is mainly used for push-to-talk voice traffic and is not able to efficiently support IP data traffic. Figure 5.2 illustrates the potential in exploiting the different communication carriers to achieve seamless communication, making the radio systems in Figure 5.1 transparent. Using the mechanisms described in [22], traffic generated by the sensors could receive a suitable service by having its own dedicated virtual topology in the common transparent network in Figure 5.2.

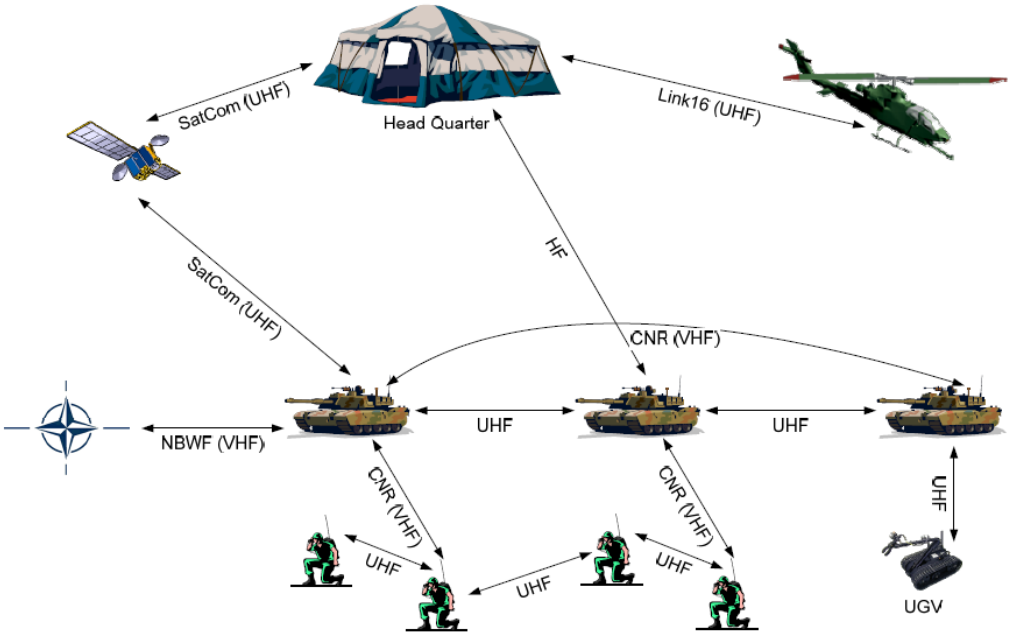

Figure 5.2 Different radio network types that might be used in mobile tactical networks (Illustration from FFI-rapport 2009/01708).

There has been a specific effort to look closer at optimizing group communication in the mobile portion of the military IP-network. Three different vignettes have been developed, which describe proposed information flows in the battalion network [23]. The vignettes describe information exchange needs for these situations:

- **Gas alarm,** where a sensor belonging to a squad detects a CWA or TIC in the surroundings. It is then critical to distribute warnings immediately to all personnel within a certain distance of the squad.
- **Hostile/Enemy artillery fire,** where the artillery makes an observation of enemy artillery attack. It is then important that the units at risk to be hit are warned immediately so they can take actions to be better prepared for the attack.
- **Medevac,** where a soldier has been wounded and needs to be evacuated out of the area. This involves both communications with an ambulance from the medical service and with a helicopter from the brigade HQ.

Fusing together the various networks in Figure 5.1 to obtain a structure such as Figure 5.2 is the focus for the work in FFI-project 1249 Network architecture for heterogeneous mobile tactical networks (*Nettverksarkitektur for heterogene mobile taktiske nettverk)*. Using IP as the interconnecting protocol, the project is developing a routing protocol to interconnect various radio sub-networks to support both connectivity and some degree of Quality of Service (QoS). A major challenge is the difference in capacity between different radio networks, spanning from a few kbps for HF radios to several mbps for SatCom.

In the FFI-project 1188 ESM in maritime common operations, and in the NATO projects MAJIIC2, it has been worked with networking of sensors for maritime surveillance. This work has identified a large operational potential in a more efficient and better suited information exchange between the tactical and operational levels, in order to give the decision makers at the operational level a more correct sensor information picture in near real time. [16].

During the work on Situational Awareness Sensor Systems (SASS), FFI has explored a low cost ad hoc wireless sensor network for use in rapidly developing situations (not CR sensors) [2]. The CR sensors are larger and will not be so widely distributed, but the ideas of sensor cooperation to give better detection rate and lower the false alarm rate could be used also for the CR sensors.

6 Discussion and further work

Whether the sensors should be networked using a dedicated network or using existing infrastructure depends on whether or not they have to be placed independent from soldiers or vehicles. If a stand-alone additional network is selected, the sensors have to be equipped with their own communication interface. Using existing radio systems, if available, would reduce the weight of the networked sensors. Lower weight will benefit both soldier and vehicle. Also, it is likely that communication resources used by the soldier are more robust and better tuned for the terrain the soldier is operating in, than a stand-alone sensor network with cheap radios. In the future we can envision that soldiers will be equipped with a set of waveforms, where the waveform best suited for the operation and traffic load will be chosen during operation planning. The mode of the network may even change during the operation to better suit the on-going operation and terrain. This amount of effort to optimize the network to the needs will probably not be done on stand-alone sensor networks.

Another place where proprietary solutions should be avoided is in the integration of the network from carrier to application. Incorporation of the networked sensors should be done by means of a standardized framework, for instance based on a Service Oriented Architecture, demonstrated in [24].

Harvesting the sensor information could be an issue if nodes are part of a stand-alone network and placed away from real time communication means. Several models for performing such a harvest, and the storage of accumulated information in the network previous to this harvesting, exist. The information could be collected using an Unmanned Aerial Vehicle (UAV), gateway nodes with other communication means, or by information retrieval when entering the area.

A sensor network may face event synchronization challenges, where the network is overloaded because of too many simultaneously triggered alarms. This is a challenge, since

CR-sensor information is very important for the local forces. Thus, alarms should be treated with high priority. At the same time, a high number of sensors would give a lot of redundant alarms, which could be smothering other important traffic. In such a case, mechanisms to sustain QoS should be incorporated, including local data aggregation and fusion.

A positive, but potentially problematic, effect of networking sensors may be that there is a desire to check sensor status more often. I.e., information that was disregarded before, such as a 1-2 bar response on the LCD, now becomes more important, since it can be correlated with other sensors. The new use of sensors may incite more frequent or more detailed information requests from the user.

Not all CR sensors should be networked in the same way as described for the LCD detectors in Chapter 4.2.1. The existing types of sensors are quite different, for example point, standoff, specialist, personal, vehicle mounted, etc. and all of these types have special needs. One could therefore think of several types of sensor networks:

- One network to handle alarms from personal sensors as described in Chapter 4.2.1. This network might also handle alarms from vehicle mounted sensors. These are not specialist instruments, and it will therefore not be necessary to transfer and store raw data from all the individual sensors. Only consolidated (fused) data need to be stored, together with some information on the number of sensors that responded, and the relative geographical positions and times of the alarms.
- One network to handle data from specialist instruments. This could be data from for example the Fuchs vehicle, where raw data need to be stored and transferred to an off-site laboratory for assistance in data interpretation. The challenges here are the sometimes specialized data format from these advanced instruments, and the existence of much larger amount of data compared to individual sensors. Flexible systems to pack the data to fit the available network capacity are therefore necessary.
- It is now more and more important to be able to answer questions relating to health and safety of the soldiers and which agents they might have been exposed to in the past. This requirement also needs to be taken care of when designing data network and data storage systems.

7 Conclusions

In order to obtain a better operational picture of CR events which may take place, it would be beneficial to connect several sensors together and fuse the information which comes from them. The sensors could be using similar or different detection principles. The networking and data fusion of information from sensors using different detection principles (orthogonal sensors) will give better information than the networking of similar sensors. The connection of both military and civilian sensors in one network will give the best possible operational picture.

The operational needs vary within the Armed Forces, but the Navy/Coast Guard shares similar needs with the Army when an exploratory team leaves the Naval or Coast Guard ship to investigate an event. Naval CR sensors are both installed and portable, and it would be advantageous for the commander to see the consolidated/fused data from all the deployed sensors together.

Different sensor networks will be needed for different purposes. Relatively simple personal sensors pose small demands on the communication resources (i.e., the network capacity), but because there hopefully will be a number of these sensors on-site during a CR event, networking these sensors would be advantageous. On the other hand, specialist instruments require larger capacity and possibly dedicated networks back to an off-site laboratory for assistance during a mission. In both cases, there will be a need to store data on a central site in an easily retrievable way, for health and safety reasons.

Another use of networked radiological or chemical sensors could be to define the boundaries of a possible contaminated area. When the soldiers identify the contaminated area, the necessary information (for example measured activity or type and concentration of CWA) is sent to the team leader in real time.

Most of the suggested solutions for sensor networks are not technologically or organizationally very challenging, but it is necessary that the CR sensors are put into an overarching architecture. It is important to take networking into account when procuring new sensor systems. For some of the existing sensors, new communication modules need to be purchased.

Existing communication networks are preferred for sensor communication, as long as the sensors are either carried by soldiers or mounted on vehicles. This will reduce the carrying weight and there will be no radio interference between the sensor network and other communication networks. However, integration of sensor information traffic into existing radio networks will require strict control with the traffic generated by the sensor network. If sensors are to be placed away from existing radios, they will have to be equipped with their own means of communication, either Combat Net Radios, or other radios forming a stand-alone sensor network. Security issues may have to be addressed when it comes to leaving a combat net radio unattended, but this may also be the case for a radio employed only for sensor communication purposes.

It is important that a central system to store and handle the data (raw data or consolidated data) is installed, in order to be able to retrieve the data at a later stage. If this is not done, one will end up with different computer systems for each sensor model, and a system where it is difficult, or not possible at all, to retrieve the data after some time.

The implemented data fusion algorithms and messages sent out from the exposed unit will be used to warn neighbouring unit and to report the incident to higher commands and should not delay immediate protective actions carried out by the exposed unit.

The CBRN community in Norway is very small. It is therefore important to make it as efficient as possible and avoid the need to retype the information at several points up through the chain of command. The data processing algorithms should only be present to assist the specialists and to speed up the warning and reporting process to other units. The specialists are always needed to interpret the data and to compare them to other available information, e.g. intelligence.

Abbreviations

AD Converter	Analog to Digital Converter
AWR	SAAB Automatic Warning and Reporting System
BMS	Battlefield Management System
Bn	Battalion
CAM	Chemical Agent Monitor
CATSS	Chemical, Atomic and Toxic compound Surveillance System
CBRN	Chemical, Biological, Radiological and Nuclear
CR	Chemical and Radiological
CCI	Command, Control and Information
CNR	Combat Net Radio
CSMA-CA	Carrier Sense Multiple Access / Collision Avoidance
CWA	Chemical Warfare Agents
DTG	Date-Time-Group
ESM	Electronic Support Measures
FFI	Forsvarets forskningsinstitutt (Norwegian Defence Research Establishment)
GIS	Geographical Information System
GPS	Global Positioning System
HQ	Headquarters
IMS	Ion Mobility Spectrometry
IP	Internet Protocol
LCD	Lightweight Chemical Detector
MAJIIC2	Multi-sensor Aerospace-ground Joint Intelligence, Surveillance and Reconnaissance Interoperability Coalition 2
MIO	Maritime Interdiction Operation
NATO	North Atlantic Treaty Organization
OODA	Observe, Orient, Decide, Act
PfP	Partnership for Peace
QoS	Quality of Service
SA	Situational Awareness
SASS	Situational Awareness Sensor Systems
SatCom	Satellite Communication
SCA	Software Communications Architecture
SCIM	Sensor Connectivity Information Management
TIC	Toxic Industrial Chemicals
UAV	Unmanned Aerial Vehicle
WSN	Wireless Sensor Network

References

[1] Forsvarsdepartementet, "Norwegian Defence Long Term Plan,"Prop. 73S (2011-2012). Et forsvar i vår tid, approved 23.03.2012, 2012.

[2] V. Pham, E. Larsen, J. Flathagen, T. Mjelde, R. Korsnes, J. Sander, and P. Dalsjø, "Sluttrapport for prosjekt Situational Awareness Sensor System (in Norwegian)," Forsvarets forskningsinstitutt, FFI-rapport 2012/02490, 2012.

[3] NATO, "ATP-45 (D) Warning and reporting and hazard prediction of chemical, biological, radiological and nuclear incidents (operators manual)," Brussels, Belgium, (NATO/PfP Unclassified), 2010.

[4] NATO, "AEP-45 (C) Warning and reporting and hazard prediction of chemical, biological, radiological and nuclear incidents (reference manual)," Brussels, Belgium, NATO Unclassified, 2010.

[5] Bruhn NewTech AS, "CBRN-Analysis, www.newtech.dk, accessed 25 July 2013," 2013.

[6] Teleplan Globe AS, "MARIA, www.teleplanglobe.no, accessed 25 July 2013," 2013.

[7] SAAB, "SAAB Automatic Warning and Reporting System (AWR), http://www.saabgroup.com/Global/Documents%20and%20Images/Land/Integrated%20Support%20Solutions/SAAB_CBRN_AWR_System.pdf, Accessed 29 July 2013," 2013.

[8] SAAB, "Automatic Warning and Reporting System (AWR), Personal communication with T. Wallin and C. Lindqvist, 20. March 2013," 2013.

[9] J. Aa. Tørnes, "CBRN-deteksjon i et nettverksbasert forsvar (in Norwegian)," Forsvarets forskningsinstitutt, FFI-notat 2008/01415 (Exempt from public disclosure), 2008.

[10] Dräger Safety Norge, "Detector interfaces, Personal Communication with Arve Sandøy on 24. July 2013," 2013.

[11] J. Aa. Tørnes, H. C. Gran, B. Pedersen, Opstad Aase Mari, P. Prydz, Ø. Wiik, and A. T. Nordahl, "Development of a Chemical, Atomic and Toxic compound Surveillance System - CATSS," Forsvarets forskningsinstitutt, FFI/RAPPORT-2004/01661, 2004.

[12] P. Prydz, "System Documentation - Chemical, Atomic and Toxic compound Surveillance System - CATSS," FFI/RAPPORT-2005/00057 (Exempt from public disclosure), 2005.

[13] J. Aa. Tørnes, P. Prydz, J. R. Nilssen, and B. Sagsveen, "Testing of the Chemical, Atomic and Toxic compound Surveillance System - CATSS," Forsvarets forskningsinstitutt, FFI-rapport 2006/02984, 2006.

[14] F. Ibsen, S. R. Sellevåg, J. Aa. Tørnes, L. H. Bjerkeseth, and A. M. Opstad, "Analyse av ukjent gass i Mathallen i Oslo 21. april 2013 (in Norwegian)," Forsvarets forskningsinstitutt, FFI-rapport 2013/01603 (Unntatt offentlighet), 2013.

[15] G. Rustad and F. Ibsen, "Observasjon av forsøk med avstandsdeteksjon i Umeå, september 2013 (in Norwegian)," Forsvarets forskningsinstitutt, FFI-reiserapport 2013/02246 (Unntatt offentlighet), 2013.

[16] Forsvaret, "CBRN-vern folder for Forsvaret (In Norwegian)," 2014.

[17] Adams J.T., "An Introduction to IEEE STD 802.15.4, IEEE Aerospace Conference, Big Sky, MT, USA," 2006.

[18] J. Li, X. Zhu, N. Tang, and J. Sui, "Study on ZigBee nrtwork architecture and routing algorithm," *2nd International Conference on Signal Processing Systems*, vol. 2, pp 389-393 (5-7 July 2010) 2010.

[19] V. Arneson, "Propagasjon i trådløse sensornett (in Norwegian)," Forsvarets forskningsinstitutt, FFI-rapport 2012/00820, 2012.

[20] C. Li, H. Zhang, B. Hao, and J. Li, "A Survey on Routing Protocols for Large-Scale Wireless Sensor Networks," *Sensors*, vol. 11, pp 3498-3526 2011.

[21] NATO, "MC 0195/9 NATO Minimum Interoperability Fitting Standards for Communications and Information Systems (CIS) Equipment onboard Maritime Platforms (NATO Restricted),"2012.

[22] M. A. Brose, M. Hauge, J. E. Voldhaug, and J. Sander, "Multi-topology routing - QoS functionality and results from CoNSIS field experiment," Forsvarets forskningsinstitutt, FFI-rapport 2013/00529, 2013.

[23] M. A. Brose and M. Hauge, "Group Communication in mobile military networks," Forsvarets forskningsinstitutt, FFI-rapport 2012/00294, 2012.

[24] J. Flathagen and F. T. Johnsen, "Integrating Wireless Sensor Networks in the NATO Network Enabled Capability using Web Services,", IEEE Military Communications Conference, MILCOM, Baltimore, MD, USA, November 7-10, 2011, pp.823-833, ISBN: 978-1-4673-0080-3 ed 2011.

[25] S. Diesen, “Manøverkrigføring i det 21. århundre: Er mekaniserte styrkers storhetstid forbi? (in Norwegian)”, Norwegian Military Journal, vol.182, no. 2, 2012.