INTEROPERABILITY BETWEEN AGENCIES AND NATIONS

Magnus WALLMARK
Ericsson Microwave Systems

Abstract: This article describes how secure and robust communications and information solutions, adapted for the National Security and Public Safety (NSPS) segment, can be obtained using commercial technology and existing infrastructure. Application areas include, for instance, emergency dispatch and command centres, agency communication and collaboration, and coast and border surveillance. The communication and information solutions follow the principles of a service-oriented architecture. The proposed approach to communications and information services for National Security and Public Safety facilitates improved operational capabilities and efficiency by providing access to much more advanced and timely information, by supporting efficient management of operations and by enabling cooperation and sharing of resources and information.

Keywords: Interoperability, Security, Network-based Defence, Open Architecture, Services.

The threat has changed dramatically during the last decade. The risk of a major war is low. We are now in a period of life in the grey-scale zone between peace and wartime situations. The authorities have to master situations involving terrorism, international criminality and participation in international missions for numerous reasons. We also need to increase our capacity to deal with post-war situations. To deal with these kinds of scenarios, variety of agencies and armed forces, as well as nations, must co-operate.

In Europe a security initiative has been launched called "Research for a Secure Europe." The initiative is already in its preparatory phase that will be followed by the main phase from 2007. The intention is to invest more than one Billion Euros per year in this research area. Particularly important is of course to decide about a kernel of standards, and some basic architectural principles. A group with that aim is also suggested in the preparatory action.

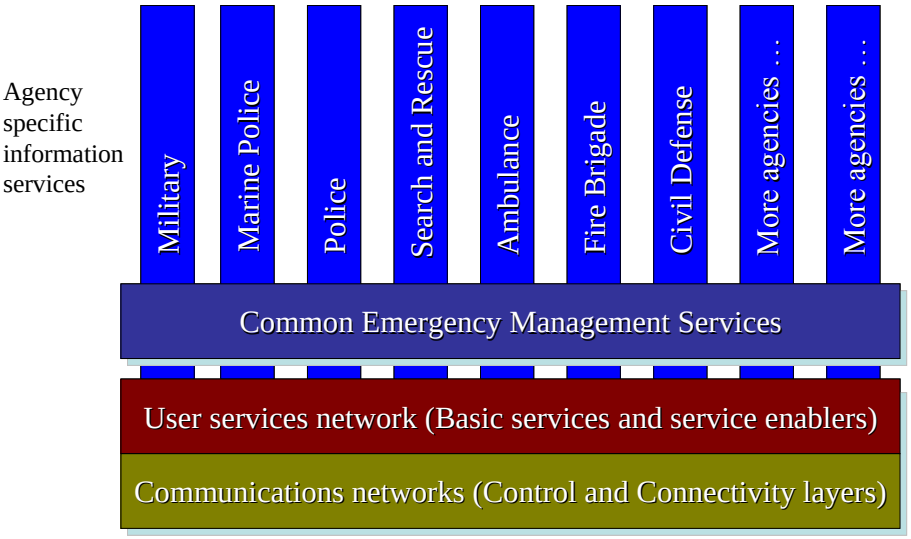

Figure 1: Security Network's Service Structure.

Ericsson supports the Swedish Armed Forces on such questions and issues in the build-up of a Network Based Defence.[1] Swedish Armed Forces emphasize that they have to be interoperable in international missions. The leadership there will normally be from NATO. Sweden, therefore, works in order to form a concept that will help to connect with NATO forces and cooperate with European authorities.

Sweden suggests the use of Open Architecture and bases the concept on commercially agreed standards. Where military standards are needed, NATO standards are preferred.

Sweden also suggests a concept based on services, which is the capability of hardware or software given an agreed standard. Sweden suggests the IP standard as it is well spread and accepted.[2] We refer to the capability as a service. Services are separated from hardware and software and may be changed independently. The concept means that more or less everything can be represented given an IP address on a network. As the services have a given standard they can easily be connected and fused or represented on each other's command systems. A car can be represented by its location directly on a map service. By clicking on the car symbol a user will get additional data of value about gas level, speed or any other service of his or her choice.

We can now form an information level built over the telecommunication networks used by a number of authorities. In analogy with Internet, they can use wireless or wire line transportation, fibre, etc., for data transfer. Sweden has decided to use IP v.6

in order to gain quality of service and a large number of IP addresses. This gives a possibility to start connecting agencies so that they can share information in real time.

Figure 1 shows three layers. At the bottom is the telecommunications layer, which transports data. Here we suggest the use of all existing telecom systems that are sufficiently good. There is in most cases a civilian infrastructure that can be used. Here we speak about tunnelling information within the system in virtual, but secure tunnels.

The next layer contains simple services that should be agreed between the agencies, such as voice, MMS, videoconference, and positioning systems. The most important layer is the layer "Common Emergency Management Services." Here simple services are combined into advanced services such as: common situational picture, geographical database, registers, decision support, etc.

A commander in the field subscribes—pulls—the set of advanced services that provide superior speed and quality in decision-making from the net. He or she will learn how to do that during exercises and in cooperation with network managers. Changing his or her toolset is easy and can be done in seconds.

This kind of build-up is also the background for international cooperation. If we can agree on a kernel of architectural rules, some of which are described above, we have a system for bridging systems and for exchanging agreed parts of information.

There need to be a handshake between commanders on what information can be transferred and which cannot. Then the digital data is labelled and sorted by nodes in the net to handle the security issue. Information security must be impregnated into the system from the beginning.

Companies like Ericsson, and others, can help nations and agencies with the technology that will make this system work efficiently and securely enough.[3] Users should focus on their operational needs. What sets of advanced services do they need in a given situation for being superior, and what methods, training, organization and manning are needed?

So now let us look at such a scenario (see Figure 2). Consider the scenario, where a fire is automatically reported over the net. An operator is alarmed and starts to feed evaluated information to the users. Through a W-LAN, the fire engine will be loaded with information already before it leaves the station. When on its way, the fire-officer starts to plan the engagement. Over the net he downloads plans of the building. The quickest way to the fire will be shown; water posts will be also located. Arriving to the fire, smoke divers go in and are escorted by a colleague who can see them in real-time in three dimensions. He can guide them to areas where a register shows that there might be persons at this time of the day. A video camera is put up to show the centre of gravity of the fire and this video information is available to everyone. The

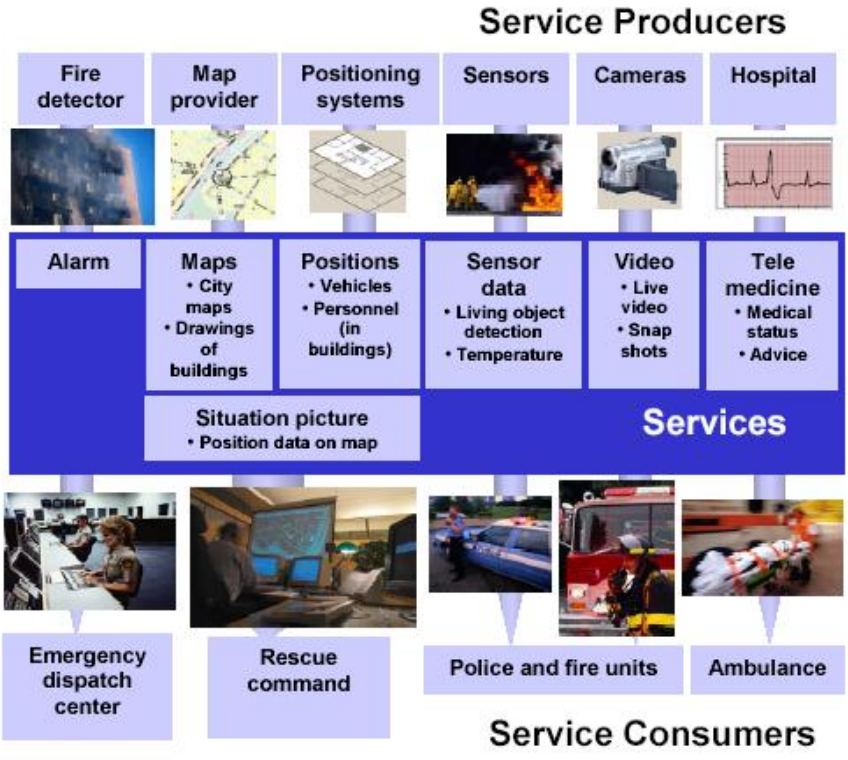

Figure 2: Examples of NSPS services and their producers and consumers. Access to services can be established at the moment a need occurs.

ambulance is guided to a safe assembly area, where burnt or wounded people are being gathered. The ambulance crew will use telemedicine devices to alert the hospital on what kind of injuries to expect. When the ambulance arrives at the hospital, preparations are already made and time is gained.

One of the most important issues is to connect agreed parts of situational pictures in real-time. Together with automatic decision support this is a base for rapid decisions. It can also be less controversial for nations and agencies to participate, as all will get a network addition. They all have their own information, but they will now also be able to use applicable information from other agencies. Over the time, the mutual trust will be increased, and more and more information will be exchanged over the network.

Certainly, there will be situations in international missions when the infrastructure in the country is destroyed or does not have the necessary capacity. Then mobile con-

tainer units can be a cost efficient and fast alternative to build a network rapidly. Ericsson response unit used by UN over the world is deployed within an hour and supports some 5000 subscribers with a network.

Many countries and agencies need support in the analysis of balancing their infrastructure for the network. Is the network secure enough? Are the principles for interoperability implemented?

There is also a need for balancing the common situational awareness picture. Present sensors need to be "wrapped" to appear as modern information services. They need to be fused with other sensors and presented to decision makers.

Ericsson is prepared to support in this respect agencies and nations in order to achieve interoperability.

Notes:

[1] *National Security Networks*, White Paper (Ericsson Microwave Systems, November 2003).

[2] *Evolution towards All-IP: the Service Layer*, White Paper (Ericsson Microwave Systems, November 2003), <http://www.ericsson.com/products/white_papers_pdf/evolution.pdf> (31 May 2005).

[3] *Communication and Information Services for National Security and Public Safety*, White Paper (Ericsson Microwave Systems, April 2005), <http://www.ericsson.com/products/white_papers_pdf/2952_nsps_a.pdf> (31 May 2005).

MAGNUS WALLMARK is Director National Security Networks at Ericsson Microwave Systems AB. He holds M.Sc. degrees in communications systems and in business. *E-mail*: magnus.wallmark@ericsson.com.