# Towards Tactical Military Software Defined Radio

Major Tapio Saarelainen, PhD, IARIA Fellow

Research and Development Division
Army Academy
Lappeenranta, Finland
tapio.saarelainen@mil.fi

*Abstract*—**This paper presents an idea-phase introduction of a tactical level communication system (battalion and below), which enables utilizing different waveforms and frequencies when communicating by using Software Defined Radio. The discussed idea-stage solution relies on using Unmanned Aerial Vehicles as hub-stations in order to ensure secure communication and reliable data transmission as regards wide bandwidth transmission to base-stations. The need for timely and accurate analyzing of the increasing amount of Situational Awareness and Common Operational Picture –related data collected keeps looming large in the battlespace. Similarly, the type and amount of different waveforms and frequencies also keep increasing. Software Defined Radio with its Graphic User Interface application, as discussed in the Results section, may offer one way of freeing the hands of a warrior to handle his or her firearm instead of a myriad of communication devices while in combat. This paper briefly looks at communication enabled by using swarms of Unmanned Aerial Vehicle and Self Organizing Networks in a military context and provisionally examines what testing and creating such a system would require and does so only at an early idea phase of a concept development process.**

*Keywords- Unmanned Aerial Vehicle, Self-Organizing Networks, Software Defined Radio/Graphic User Interface.*

## I. INTRODUCTION

This paper presents an idea-phase introduction of a tactical level (battalion and below) communication system to be used by a tactical end-user performing in a battlespace. As this paper's contents represent an early idea stage of concept development, the system drafted and its features described have neither been operationalized nor field-tested. When creating any new functional system, the first step of the development process concerns outlining an idea of what a functioning system necessarily needs to comprise. This idea phase of a concept development process turns into a fully-fledged concept with operationalized features to be tested once the end-user devices discussed in this paper have first been brought into being. Testing the devices described in an environment similar to what the paper outlines requires resources, i.e., political decisions allowing funding, personnel, and time. Any testing in lab conditions becomes impossible as no combat settings can be neither operationalized nor modelled in laboratories.

The key issue in modern warfare continues to be communication. Without communication there are neither coordinated operations nor success. High Data Rates (HDR) are needed for the type of data necessary in Battle Management Systems (BMS) and in Command Posts (CP) where operations are commanded and controlled and orders issued onwards for tasks to be executed by lower echelons.

Military environment is challenging also from the perspective of communications. Hostile military environment possesses challenges of several types for the need to communicate. First of all, the communication environment, a battle zone, is hostile. An adversary party tries to deny the free use of the frequency spectrum. Similarly, attempts of jamming the adversary's communication devices are typical of military actions executed in different frequencies and waveforms in the battlespace. Secondly, the soldier operating in a hostile territory using Cognitive Radios (CR) needs to establish mutual contact by using CR equipment to forming an ad hoc network. The challenge to create a functioning network in this case is exacerbated by the likely lack of accurate knowledge of the usage patterns of a radio spectrum in the hostile territory. If we compare this situation with a civilian case, where the frequencies and platforms are known in advance, the challenge in the military case has to be solved somehow in order to create a functioning communication network.

This paper introduces the challenges of the Future Force Warrior from the perspective of a consumer of communication services. This issue is essential for both the research community and the relevant industry. Once problems are pointed out, the process of finding solutions is easier. This paper presents one solution for how to facilitate fighters' need for constant capability to communicate in the battlespace.

This paper examines tactical level military operating referring to commanded tasks being executed at the level of company and below. Both soldiers and commanders of any kind are dependent on radios to execute missions. A single soldier relies on radio communication in order to be commanded. This asks for a reliable communication tool and a robust ubiquitous network system that allows for precision and minimized collateral damage. A battlespace can be understood as an environment, where operations are being executed including land, sea, air, underwater and cyber

operational environments. Warriors, sensors and Unmanned Vehicles (UVs) of several types operate and communicate in the versatile, constantly changing battlespace. As indicated in [1], militaries are using sensors as part of their battlefield strategy. As mentioned in [1], the integration of data collecting capabilities is in an essential role in expanding the communication platform capabilities. The key issues involve collecting the data, analyzing these data, and forwarding the analyzed data reliably and in an intact form to the end-user, a Future Force Warrior (FFW). Networks have to be organized to cover the needs of the end-user at all levels, as explained in [2]. Issues such as Quality of Service (QoS) and Speed of Service (SoS) are seminal in tactical communications [2].

Militaries concentrate on sustaining and developing their capability to communicate in a battlespace. To optimize performance, a Future Force Warrior needs only one communication device, which can be Software Defined Radio (SDR) for the reasons listed. First, one communication device covers all the communication needs of an FFW instead of him or her needing to use several communication devices. The focus of the FFW has to be in fighting. This means that an FFW keeps his or hands around the weapon, monitors the threats in the battlespace and fights. Secondly, mobility- and action-critical matters from the perspective of an FFW, such as size, weight, and power and cost (SWAP-C), are relevant. Thirdly, one power source should cover the need of communication devices instead of several sources (i.e., power source for radio and Personal Digital Assistant). Lastly, one communication device will ease the communication burden of an FFW and he or she can focus on the main functions: to monitor the environment and fight to survive. Present military communications are based on combat net radios (CNR), dominated by the enhanced position location reporting system and the single channel ground and airborne radio systems. This means that the varying levels of tactical communication can comprise several actuators. The distances between the communicating elements can vary from only a few meters to tens of kilometers and more. Tactical communication utilizes unmanned vehicles, drones and satellites acting as hubs or relay stations. The term tactical refers to the operative capabilities of a given military force. For example, a maneuver, which is tactical for the U.S. Army with its special forces, can be an operative maneuver for an army smaller in size and its operative capability.

The basic problem in communication is that the High Data Rate gives shorter range in communication (e.g., 4 x rate = ½ range). Therefore we have to solve this problem with different means than just increasing the data range with increased transmission power. Despite the system characteristics, the communication system for military use in lower echelons (i.e., companies and below) has to fulfil the requirements of operational security, coverage, connectivity and Low Probability of Detection (LPD) and Low Probability of Identification (LPI). Military operations are dependent on covert high-speed networks, which also represent functional requirement of modern infantry and special operations warfare [3].

This paper introduces a solution utilizing a swarm of Unmanned Aerial Vehicles (UAVs) and SDRs. The swarm of UAVs is seen as a platform for a communications system, in which the distances between the UAVs must be short to ensure the message throughput in a hostile communication environment. This aims at ensuring a reliable data exchange process and fulfilling the requirements of LPD and LPI. SDRs are used by FFWs performing at the tactical level and also embedded into each UAV to ensure a reliable data exchange process. The swarms of UAVs in this system are in a central role to ensure the message throughput in a case when one or several UAVs are destroyed. Once a UAV becomes incompetent to act as a relay-station, a neighboring UAV takes over its functions and, with the assistance of Self-Organizing Networks (SON), the routing of communication can be reorganized and ensured.

This paper is organized as follows: Section II discusses Military Communication Environment, Section III focuses on the Challenges of FFW, Section IV introduces SDR, Section V introduces Universal Software Radio Peripheral (USRP). Section VI concentrates on explaining the idea of Cognitive Radio (CR). Section VII discusses the significance of a Graphic User Interface, and Section VIII introduces the new system. Section IX examines the strengths and weaknesses of the introduced system and Section X concludes the paper with Section XI describing the demands for future work.

## II. MILITARY COMMUNICATION ENVIRONMENT

Military communication environment differs from its civilian counterpart. Any civilian communication environment tends to be non-hostile and its features thoroughly known in that the transmission distances, frequencies and waveforms used are common knowledge. In contrast, the military communication environments are part of a battlespace and abound in uncertainties in connectivity and latency may vary uncontrollably due to incessant hostile electronic warfare attempts. Communication break-down in a battlespace typically results in compromising someone's life. A given battlespace comprehends also the communication environment, in which war is waged. Military frequencies tend to be mandatory and always commanded from higher echelons in order to control the electromagnetic spectrum most effectively from the execution perspective of own military operations.

Military troops equipped with varying end-user devices transform the battlespace of 21st century into network-centric warfare with Network Centric Operations in a central role. SDRs will provide a flexible tool suited for the changing military environments in that they allow versatile communication in the battlespace [4]. In a constantly changing battlespace the commanded troops can be mobile or static. Often the communication tools, end-user devices, are handheld and lightweight. A ground level military performer, soldier, has to be able to communicate also via satellites in order to contact higher echelons, for example, when executing special operations in rocky terrain. The size of the used system, together with its weight, power and cost

(SWAP-C) become vital from the perspective of the system user and provider.

For the end-user, to be able to cover multiple battlespace scenarios, the simultaneous requirement of communication requirements such as voice, video and data together with the capabilities and megabit bandwidths set design challenges. Moreover, to sustain secure communication by means of the end-user devices, new military waveforms have been designed to fulfil the requirements of the end-user, a soldier. An example of such waveforms suitable for an SDR-based system implementation is WiMAX 802.16e, which has been modified to operate in the military frequency range of the NATO UHF band of 225 – 400 MHz [5].

A future military SDR-platform should support multiple radio frequency frontends. Depending on the available and sufficient frequency bands, different frontends could be installed. The flexible use of different frontends and waveforms enable finding a suitable system configuration for all the planned operational scenarios. The next generation SDR-based platform should enable at least the following benefits for tactical networking: First, mobility support for mobile ad hoc network (MANET). Second, sufficient communication capacity must be guaranteed at the tactical level, this is a minimum throughput of 1 Mbps to support mobile user. Third, from a perspective of life cycle management, a SDR platform must be independent from the waveforms and frequencies used. Fourth, communication flexibility has to be ensured with radio frequencies in SDR frontends and with used waveforms. Fifth, interoperability with national and coalition waveforms has to be granted [5].

In a civilian communication environment an end-user can benefit from reliable and fast communication, high throughput of messages, issues of low latency, the constant capability to communicate, adequate bandwidth, good Quality of Service (QoS), and Speed of Service (SoS). Civilian communication systems offer the possibility to benefit from constant power supply or the capability to recharge the battery of the used communication device when necessary. The communication process usually suffers from only slight if any hostile interference or jamming.

Communication systems utilized in a military environment can confront all types of interferences. These include jamming and all means electronic warfare with a constant threat of becoming annihilated by the adversary if a communication tool has been detected, pinpointed, and placed in the targeting process to be destroyed. Table I lists the differences between civilian and military communication environments.

TABLE I.        DIFFERENCES BETWEEN CIVILIAN AND MILITARY COMMUNICATION ENVIRONMENT

| Characteristics of Communication | Military communication environment | Civilian communication environment |
|---|---|---|
| Free use of spectrum | Restricted | More possibilities |
| Latency | Varying, sometimes high | Typically low |
| Energy | Limited, hard to recharge | Possibility to recharge fast |
| Hostility | High | Low |
| Jamming | Possible | Low |
| Adequate bandwidth | Limited, altering | Typically high |
| Limitations in use | Often restricted | No limitations |

As Table I indicates, in a military communication environment the characteristics of communication involve restrictions and constant uncertainty due to hostility in the battlespace.

## III.    CHALLENGES OF FFW

The following overview lists six challenges which have been identified within the military community. The writer has encountered these challenges while conducting research on related issues, such as a nationwide Company Attack Study performed during 2004 – 2007 in Finland. The first challenge is related to the main task of a fighter: the main task of an FFW is to fight in performing the given mission. This means he or she has to monitor the environment to stay alive and to be able to execute the commanded tasks. He or she engages the enemy with all the weaponry available. This also means that the FFW relies on connectivity and capability to communicate at all times. The constant connectivity poses the second challenge. Mission success requires the capability to transmit and receive data and commands. The constant communicating ability requires that a single warrior be capable of acting as an executor of an operation, or a military commander at some level. Connectivity remains the key. Some sort of a network must be available at all times. Location data and commands can be forwarded only by means of a functioning network and a reliable hand-held or soldier-mounted communication device.

The third challenge is linked to the usage of warrior platforms. A warrior platform consists of several subsystems and their control units. For example, the systems can be controlled via a wrist-worn user-interface presented here. All the communication controls can be easily and rapidly found from the wrist-held device which is embedded onto the arm and acts as a supporting hand when using a personal firearm. Contrary to a visor-embedded system, this wrist-held device

does not hamper viewing the environment with a constant data flow. Figure 1 features a wrist-held device.



Figure 1.  A wrist-worn control system into which SDR can be embedded.

The fourth challenge involves the number of networks and data sources on which an FFW relies. If the communication network or operating unit malfunctions, FFWs get in trouble because they lack the necessary resources either because of the different frequency of waveform used or the network becoming out of coverage. This slows down a single FFW and usually harms the whole military operation.

The fifth challenge equals the access to different types of Battle Management Systems (BMSs). BMSs support the efficient utilization of military units at all levels. The access process into a BMS requires more bandwidth than using voice and text messaging when issuing commands. Figure 2 features BMS.
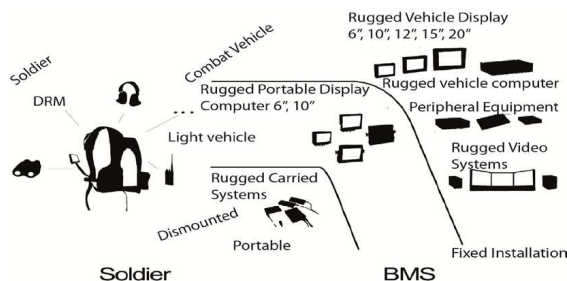


Figure 2.  Soldier Systems linkage into Battle Management Systems.

This sets more bandwidth demands for SDRs used. The data may surface in varying waveforms and frequencies. In order to benefit from BMSs, the location and identification of friend or foe are relevant. These data are needed from the battlespace to ensure the effective use of different weapon systems.

Systems related to location data and identification systems keep improving. The command and control capabilities necessary for units serving at battalion level and below are provided by means of BMS. Present combat net radios can only be seen as beneficial tools in supporting geographical based situational awareness. When several operational BMSs are integrated, it is possible to maximize the amount quantitative and qualitative data for analysis purposes. This involves applying the concept of System of Systems (SOS) and utilizing robotic platforms. The sixth challenge is the type of a Graphic User Interface (GUI) of a

communication device, which can be used for various purposes. GUIs can be utilized in creating the Situational Awareness and Common Operational Picture as well as for location services and for weapon selection process. Although one of the challenges is the variety of used waveforms and the bandwidths, they fall outside of the scope of this study. This paper discusses a possible solution for the listed challenges.

## IV.  SOFTWARE DEFINED RADIO

SDR is a radio communication system in which components that have typically been implemented in hardware, for example, mixers, filters, amplifiers, modulators/demodulators, and detectors, are instead implemented by means of software on a personal computer or embedded system. Usually SDR can be programmed to support frequencies from 100 MHz to 6 GHz with using 130 nm Complementary Metal Oxide Semiconductor (CMOS) technology [6]. Depending on the system configuration, typically supported signal bandwidths can vary between 700 kHz and 40 MHz or 200 kHz and 40 MHz, depending on the CMOS used [6]. In other words, SDR is a wireless communications system where the traditional hardware is replaced by software modules [7]. While the concept of SDR is not new, the rapidly evolving capabilities of digital electronics enable executing many such processes which earlier used to be only theoretically possible.

Currently, most SDR related products and studies focus on analog communication and voice transmission. The SDR platform consists of Field Programmable Gate Array (FPGA) -based radio hardware and open source SDR software module [7].

The main features of SDR include: 1) radio spectrum sensing; 2) reconfigurable radio modules and 3) link for digital data communication. These features form an important basis to accomplish Cognitive Radio technologies.

The mobile devices can afford the high speed and complex computation owing to the advance in computing ability of the processor, such as Personal Digital Assistant (PDA), Smart Phone, or Ultra-Mobile PC (UMPC).

Most of these mobile devices equipped with Wi-Fi, WiMAX or other wireless modules enable end-users to access services anywhere. The traditional hardware radio system comprises a variety of analogy elements such as filters, converters, modulators and demodulators. The hardware is expensive and has low compatibility with other components.

The reason why SDR becomes increasingly popular is that it allows using SDR technology for realizing many applications relatively effortlessly in the integration of different components. The most used software architecture for SDR is the Software Communications Architecture (SCA), which is considered as the standard for military domain [4]. The novelty of SCA lies in the availability of SCA-based tools to allow designers to create component-based SDR-applications as assemblies of components and logical devices. When these types of systems are being created, the communication between the components and devices must be carefully orchestrated. In this process it is

possible to benefit from the use of Common Object Request Broker Architecture (CORBA) [4].

When discussing SDRs, security issues must be considered. When new Software (SW) is being loaded, the consequent threat of having unauthorized and potentially malicious SW installed on the platform becomes possible, if security precautions have not been taken, by, for example, adding a digital and verified signature in the code before the new software is being transmitted.

In order to successfully benefit from the products and performance of SDR, we have to focus only the performance produced via SDR. The added value from SDR can be seen via tactical communication requirements for the FFFW operating in Battlespace which are: Situational Awareness (SA), Common Operational Picture (COP), Command and Control systems, identification friend or foe (cf. Figure 3. below), (IFF)/Blue Force Tracking, capability to co-operate with UAVs and Unmanned Ground Vehicles (UGVs) and robots, data from sensor to shooter, Voice, Navigation, messaging, Imaging, Video, Security.

One interesting possibility is to embed Radio Frequency Identification (RFID) system into SDR by using Quadrature Amplitude Modulation (QAM). The system has been explained in [8]. The identification friend or foe (IFF) process can be embedded as part of SDR functions. Figure features 3 an IFF process.
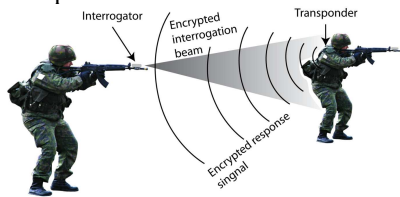


Figure 3.   Identification process Friend or Foe (IFF) in progress.

By simply downloading a new program, a SDR is able to interoperate with different wireless protocols, incorporate new services, and upgrade to new standards. One solution is depicted below above while the process is introduced in Figure 4.
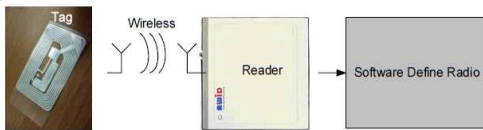


Figure 4.   RFID system with SDR [8].

As Figure 4 indicate, by combining the Radio Frequency Identification tags and IFF –process it is possible to decrease the total mass of the gear a FFW carries. Similarly, this enables simultaneously decreasing the amount of transmission energy necessary for identification purposes. RFIDs can be sensitive to electromagnetic interrogation signal by nature and need little energy when responding once only a slight transmission signal focuses on them. Thereby the amount of response energy transmitted towards of the interrogator can be significantly small. This means Low Probability of Detection as regards the surveillance tools spread in the battlespace. Relevant for operational security

purposes, the interrogation process remains undetected and discreet.

## V.   UNIVERSAL SOFTWARE PERIPHERAL RADIO

In Universal Software Peripheral Radio, we examine only the functionality of USRP. In doing so, we notice it offers more performance than its predecessor SDR. The technology used in USRP is located in the hardware implemented in frontend for sending and receiving waveforms. USRP offers different frequencies, bandwidths and frequencies for specific purposes. The USRP can be fixed to respond to the end-users' requirements by selecting appropriate motherboards for controlling the frequencies and waveforms [7].

USRP can be divided into two parts based on the transmission path. These are the transmitting signal path and receiving signal path. For example, on transmit signal path, users can define the setting parameters by software on personal computer such as radio protocols, modulation types, frequency of spectrum modulation.

Then the USRP receives the parameters, and FPGA executes Intermediate Frequency (IF) processing on Digital Up Converter (DUC) and Digital Down Converter (DDC). After the Intermediate Frequency process, users adjust the baseband to the frequency band selected before.

The last step on USRP motherboard is that digital to analog (DAC) converts the digital signal into analog signal. Finally, the analog signal is transmitted to the antenna through the interface side on the daughterboard, as illustrated in USRP block diagram in Figure 5.
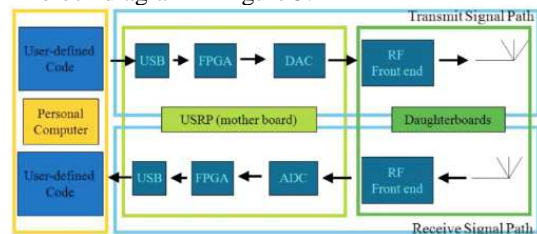


Figure 5.   Composition of USRP [7].

As Figure 5 demonstrates, the composition of the introduced USRP system offers flexibility in using different waveforms and frequencies. The flexibility can be offered by different daughterboards which can be tailored to meet the requirements of different frequencies and waveforms. By changing and tuning the performances of daughterboards, the FFWs have improved communication devices as communication tools in a constantly altering battlespace and varying missions.

## VI.   COGNITIVE RADIO

When moving on towards the communication device suitable for an FFW, we have to take a quick glance at Cognitive Radio (CR). As widely known, Software defined Radio is a platform for Cognitive Radio [9]. Without going into the details of the technical structure or composition of CR, we focus on the listed and wanted end-products and functionalities of the CR from an FFW perspective.

Cognitive Radio capabilities and functionalities include the following features. First, Spectrum Awareness (SAw), which means being able to detect quickly and robustly the presence of incumbent (preemptive) users to avoid causing interference. Second, Dynamic Spectrum Access (DSA), which means CRs will access the spectrum on an opportunistic basis. Third, Dynamic Spectrum Sharing (DSS), which means CRs must be aware of other CRs' coexistence. Lastly, CRs are Spectrum Agile (SAg), which means that CRs should provide seamless operation over multiple channels. Also challenges related to adaptive coding, modulation and multi-access have to be solved as indicated in [9].

There is a long way towards CR, which meets the listed requirements. From the perspective of an end-user, a consumer, an FFW, it is essential to meet the requirements listed. This also applies as regards the scientific community and the industrial community. The necessary requirements have to be identified prior to being able to produce a wanted end-product.

One solution for designing the suitable architecture and configurations for the future force radio communication device could be Software Communications architecture. SCA has been created to assist in the development process of SDR communication systems. SCA allows for waveform application software to be more easily ported across radio platforms. At the moment publicly available specifications can be found for SCA 2.2.2 and 4.0, as well as for SCA Appendices and SCA APIs. As a matter of fact, it is possible in next generation products to take full advantage of the following: First, SCA 4.0, which is to empower more freedom to do the SDR implementation. Second, Programmable SDR chip sets. Third, offering more efficient SDR development tools and use of more efficient higher level modelling methods. Fourth, adding a new approach to waveform portability and full utilization of SDR work done in commercial domain. Lastly, designers are focusing on developing of sophisticated RF front-end technologies.

SOA -technology involves assisting processes performed in military operations. As indicated in [10], the SOA has been used to design and construct the CR systems. When an FFW can benefit from the possibilities offered by a successful adoption SOA, also in communication services, the result can be improved overall performance in military operations.

Figure 6 features how the data are gathered, processed, analyzed and then transmitted as commands to an FFW. If the data are correctly collected, analyzed and successfully transmitted to the performer, an FFW, the process of waging war can be improved and collateral damage minimized. Various battlespace sensors transmit data to a context-aware reasoning layer. In this layer, data are converted to context and an inference engine transmits the data to a ubiquitous main layer for analyzing purposes. The data are verified, analyzed and transmitted as information for the execution of the operation [11]. This process is depicted in Figure 6.
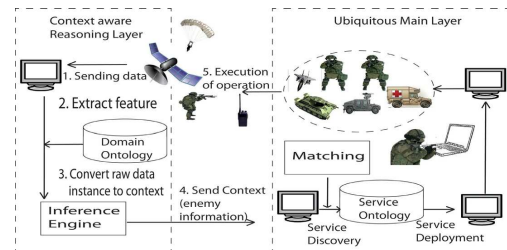


Figure 6. Increased FFW performance can be gained via successful data utilization and analyzing process [11].

Once the collected data have been analyzed, they can be forwarded to the military performers who need these data most. The transmission process has to be automated to ensure sustaining soverall performance.

## VII. GRAPHIC USER INTERFACE

A new type of communication device for an FFW has to fulfil the specific communication needs of an FFW. The communication system and the GUIs have to be defined to fulfil the needs. Figure 7 features the actuators affecting the system definition process.
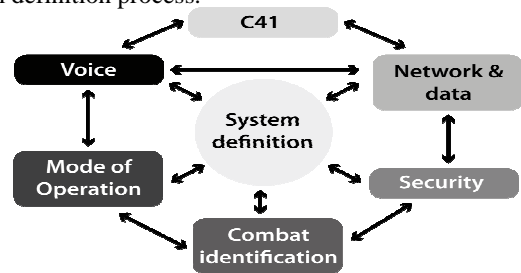


Figure 7. The idea of configuration of the future communication device from a perspective of a consumer, an FFW.

According to results presented in [12], the visualization of events can improve the human capability to accelerate the Military Decision Making Process (MDMP) by offering necessary information in required time and understandable form. From the perspective of a consumer, an important role is set for the type of a GUI. A functional GUI is a means to present collected data, a control panel to access networks and guide UVs, a tool for a weapon selection process, and, of course, a communication tool for the entities of higher and lower echelons. Figure 8 features one possible figure caption of a functional GUI.
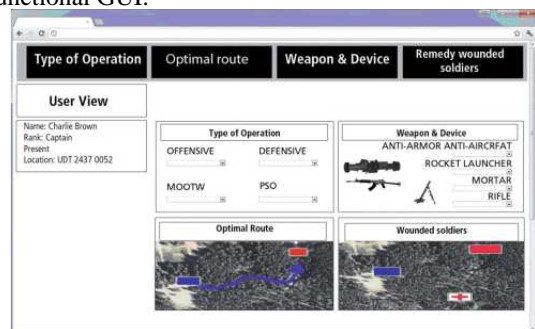


Figure 8. A wiev of a Graphic User Interface.

Apart from the mentioned facts, an FFW has to be able to access BMSs of various types and different databases with a new type of communication tool. Figure 9 features one type of BMS where an FFW can be constantly connected to optimize the performance while executing tasks.
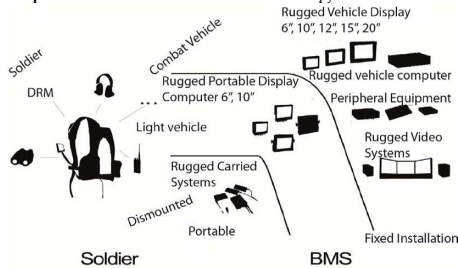


Figure 9.   A wiev of a BMS.

Lastly, an FFW has to be able to control the systems embedded on his Battle Dress Uniform (BDU). Figure 10 below features the FFW's electronic skeleton and its functions [13].
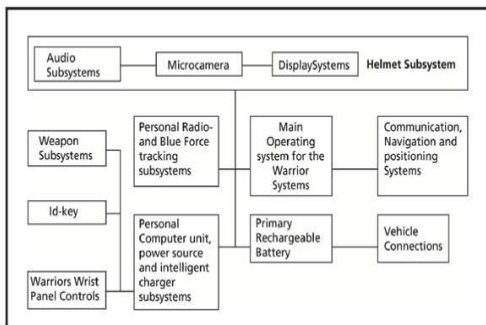


Figure 10. A composition of a FFW's electronic skeleton [13].

An FFW uses the control unit embedded into his BDU as an essential tool to control and monitor the functions of own gear. In Figure 11 below, the controlling system is wrist-worn.
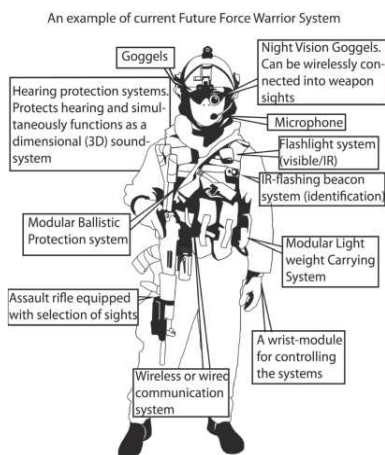


Figure 11. An example of an FFW as a platform with selected gear [14].

By embedding all the control units of the FFW's electronic gear into one wrist-worn controller, the number of controlling units can be decreased. This may increase the overall performance of the FFW as the FFW can find all the control units in one location instead of needing to separately control each different embedded system listed in Figure 11.

## VIII.   A NEW COMMUNICATION SYSTEM FOR THE FFW

As noted in [3], mobile ad-hoc networking of dismounted combatants is necessary as regards the future involving net-centric operations. The amount and variety of data transmitted in the battlespace keep increasing. Issues such as bandwidth, type of waveform, frequency and security are only a few of the issues that have to be accounted for. Low Probability of Detection and Low probability of Identification remain critical in covert operations, as mentioned in [3]. Single UAVs are utilized as tools tailored for Special Forces and a system relying on Advanced Encryption System (AES) encrypted network with a range of 3 kilometers [12].

A new communication system is possible to create if we utilize the capabilities of SDR, swarms of UAVs, SDR and Self-Organizing Networks (SON) implemented in 4G networks. It has to be highlighted that in this system, SDRs are implemented in FFW gear and inside an UAV. As noted, SON aims to configure and optimize the network automatically, in a manner that the interaction of human can be reduced and the capacity of the network can be increased.

The main functionality of SON includes the following: self-configuration, self-optimization and self-healing. SON is described as a part of 3GPP LTE and it is a key feature for effective and automatic operation and maintenance (O&M) of 4G networks. Besides that, SON maximizes overall performance of network and reduces the cost of installation and need of management by simplifying operation and maintenance through self-configuration, self-optimization and self-healing. SON also reduces the power consumption and results in reduced operational expenses and produces an environmentally friendly approach. Figure 12 features the SON as seen in [16].
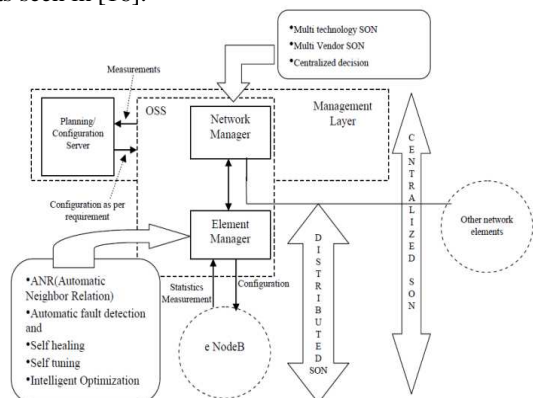


Figure 12. A composition of a SON implementation in 4G as seen in  [16].

When a swarm of UAVs is utilized, the distances needed to communicate with an FFW-worn SDR must be minimal in order to ensure the message throughput in this system.

Different types of data can be transmitted from a soldier to a higher echelon via an UAV. Security issues remain essential when dealing with UAVs utilized in Network Centric Warfare at a tactical level. This means opting for low transmission power and thus minimizing the chances of the UAV becoming detected, targeted, and destroyed.

When transmission distances remain short between the ground (FFW) and aerial stations (UAV), the accrued and transmitted data can be better secured and requirements of LPD and LPI can achieved. When SON utilizes all the SDRs, those embedded into the UAVs and those embedded into soldier worn systems, this data exchange can be executed successfully and thus ensure that the data remain intact and coherent. Figure 13 features the data-exchange process via a command post and UAVs with the assistance of embedded SDRs into the mentioned entities.
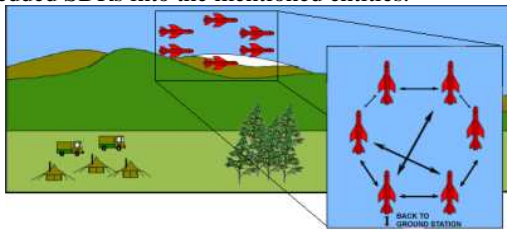


Figure 13. A data exchange process with the swarm of UAVs.

The swarms of UAVs will forward the data automatically via the network system created by UAVs. Demands of LPD and LPI can be fulfilled, because the transmitting energy used via the transmission protocols by means of UAVs remains low.

IX. DISCUSSION

A military environment, battlespace, differs from a civilian environment. In battlespace both constant stress and uncertainty continue to dominate. The fear of losing one's life prevails. An FFW has to monitor his or her environment when fulfilling the commanded mission and stay alive. The mental capacity of an FFW must be focused on the matters at hand. The lower the number of gadgets an FFW has to monitor, the longer his or her life with an increased possibility to continue performing.

Militaries aim at developing SDR into a communication tool for all the troops at the tactical level. The process of embedding a functional SDR as part of military troops' communication devices is still globally ongoing in militaries, with no existing, operationally fully functional end-user devices anywhere in combat use able to transmit large amounts of data in various waveforms and frequencies. Meeting the requirements of mobile users in a battlespace remains challenging. Issues related to SWAP-C have to be solved. One critical challenge related to military SDR use involves achieving sufficient computational capacity. This is a problem when processing wide-band high-bit rate waveforms consisting large amounts of data. In terms of SWAP-C, an FFW needs the selected communication end-user device to be reasonably tailored with optimally minimal total mass of a device, its batteries and recharging units. This means that Data Processing Units (DPUs) and Event Driven

Administrative and Control Components (EDACCs) have to be carefully selected and orchestrated to meet the operational requirements of the end-user [7].

The issues related to energy cannot be over emphasized. The energy requirement of a typical handheld device can be between a few hundred milliwatts [15] to few Watts [8]. The system specifications of the SDR are significant in defining the energy needed as well as the amount of data transmitted.

Challenges related to operational security are essential in reconfiguring the SDR-systems, especially as regards software. While loading a new program, new waveform or new hopping sequence, issues of transmission security during the different uploading processes have to be guaranteed. If this part becomes neglected, the SDR will not act as a useful tool in own hands in net-centric operations but rather becomes a novel tool to be exploited by the adversary.

A communication system that serves fighters' needs is creatable if we utilize the capabilities of SDR, swarms of UAVs, SDR and SON implemented in 4G networks and combine them as depicted in Figure 13. This means that an FFW's end-user device, SDR, is connected with a swarm of UAVs via SON. The swarms of UAVs form an own data communication system in which the data transmission distances between UAVs are short and operationally secure. This in turn will fulfill the requirements of LPD and LPI. The described delicate system introduced is a new one and based on ideas that can be executed by utilizing existing Commercially Off-the-Shelf (COTS) technology. The system is not yet bullet-proof and can malfunction for a number of reasons. Challenges related to creating the described system have to be solved to enable the function of different processes. The orchestration of the system can also fail because of intentional enemy action (jamming, a virus, a worm). The system needs to be equipped with an analyzing program, which indicates when the system functions properly before using the system. This asks for an easily replaceable and fault-tolerant system with inbuilt check-in routines. Otherwise, traditional methods in orchestrating services need to be adopted.

The introduced system offers an access to communication processes, which are created to support command and control systems. An FFW relies on communication services. To enhance SA and COP, it is essential to have user-friendly GUIs of some kind for presenting data. As noted, time remains a critical factor in tactical-level operations and the main function of an FFW is to fight, not to spend time browsing different databases in search for vital data.

Creating a new communication tool requires resources, such as personnel, time, money, troops and space to execute the use of the tailored device in pre-defined drills. The vendors and the end-users have to co-operate to create a functioning communication and control tool for the use of an FFW. In the development process, the use-cases and usage methods of SDRs have to be defined. This includes defining use-cases of operations, training-scenarios, types and timing of operations, training practices, data gathering during the exercises, and After Action Reviews (AARs) together with debriefing-sessions for system designers and troops after

implementing the training-scenarios. The system-creation process requires strict timing in a well-orchestrated series of field testing in which the system users and system developers have to attend the tests at the same time. The time required for field testing equals approximately a decade, the number of training drills necessary a hundred, and the number of military personnel committed to executing the drills a hundred. The complexity of the SDR system requires that a handsome number of designers and engineers from the vendor's attend the drills, ideally one on one. The estimated funding requirements equal at least a 100 M€. However, only average ballpark figures can be estimated as the actual realized costs and their approximations would by default value be labelled classified. The number of personnel and funding required described in this paper rely on the experience accumulated over twenty years on active duty as a field-test participant. The military personnel, designers and engineers have to be fully committed to this work in order to achieve results. Table II below lists the identified resources needed for the described study. In order to create a feasible testing system, an amount of work equal to producing a dissertation is required.

TABLE II.     ESTIMATED RESOURCES TEQUIRED FOR FIELD-TESTING

| Types of resources required | Vendor side | Military side |
|---|---|---|
| Money | 30 M€ | 70 M€ |
| Personnel | 100 | 100 |
| Time for planning | 2 years | 2 year |
| Time for testing the system | 5 years | 5 years |
| Time for evaluating the results and the system | 2 years | 2 years |
| Reserve time | 1 year | 1 year |
| Total resources | 10 years and 30 M€ | 10 years and 70 M€ |

Table II features only a rough estimate. More precise data requires pre-planning for a period of twelve months. Different sources of funding, such as industrial and / or academic contributions of personnel and / or equipment, need to be estimated before any final estimation is doable.

## X.     RESULTS

The main result is an idea-phase introduction of a tactical level (battalion and below) communication system to be used by a tactical end-user performing in a battlespace. As this paper's contents represent an early idea stage of concept development, the system drafted and its features described can neither be operationalized nor field-tested.

An FFW performs in a battlespace filled with ubiquitous networks and communication systems. He or she has to cope with actions involving humans and machines, such as databases and UVs. Equipped with a reliable communication tool, an FFW can perform tasks with improved speed and efficiency. Bespoke SDR can enhance the performance of an FFW by answering the defined challenges listed in Section III.

To sustain optimal performance, an FFW has to be able to use only one single device for command and control. This device can be an SDR with a GUI. This way there is only one single device, Software Defined Radio/Graphic User Interface (SDR/GUI), for an FFW to communicate and use controls with instead of being exposed to several communication tools. Compared to a stable civilian environment, a military environment equals a constantly altering battlespace. An FFW has to be able to monitor the events in the prevailing environment instead of needing to update the status and monitor his or her command and communication tool. An FFW has to have hands on a weapon and be ready to act when necessary. If unable to do so, the FFW will become incapacitated by a splinter or a bullet. It is essential to enable an FFW to receive and transmit data with the assistance of SDR/GUI, into which SDR can be embedded.

First, an improved SDR/GUI can act as a control-station for all of the digital systems. This allows an FFW to focus on his or her main task, to fight. He or she can monitor the prevailing environment and use his or her weaponry in a time-critical environment. Second, an FFW can concentrate on one device, SDR/GUI, instead of monitoring several screens and displays. He or she saves time and can focus on the task commanded. Third, the control units of his or her own warrior skeleton and communication controls can be found from one communication device, SDR/GUI. The fourth challenge can also be solved by adopting SDR/GUI which will take care of the various networks and waveforms and switch automatically to the free and appropriate channel to transmit or receive data.

The fifth challenge was a problem concerning the access to BMS via different communication tools. The problem is linked to the issues of bandwidth, frequency and waveform. The accessing process into BMS involves utilizing the performance provided by the SDR and SON. This means offering the frequencies, bandwidths and waveforms required from the fighters' perspective. The swarm of UAVs serves as a secure and replaceable communication gateway for the data exchange process. This allows for keeping the transmission power low and transmission ranges relatively short. The Sixth challenge was linked to the GUIs. To comprehend the prevailing operational situation and a holistic list of events at a tactical level, an informative presentation of SA and COP is in an essential role. The presented system together with improved SDR/GUI can be seen as a feasible solution to solve all the listed challenges. Figure 14 features a possible view of a functional SDR/GUI for the FFW operating at low level (company and below) tactical operations.

Figure 14.  An example of tactical SDR/GUI.

Tactical SDR/GUIs can serve as command and control tools offered for the FFWs. SDR/GUIs can be utilized as tools for possibly enhancing the overall performance of the soldier. An FFW needs only a short period of time to take a look at the SDR/GUI and notice if something significant has changed in the overview. An FFW can concentrate on his or her main mission, which is to fight instead of constantly monitoring all the controlling units of his or her gear.

## XI.  FURTHER WORK

When moving towards tactical military SDR/GUI, the system presented requires funding and field testing to be able to create a functional end-product. The rough estimate of the resources required is evaluated above in Section IX and in Table II based on the experience gained in twenty years spent as a participant in different military tests. Automated systems and allocation of diminishing resources force militaries to consider the facilitated performance offered by means of exploiting SDR/GUI. The result could be an agile and modular military performer with ever-improved capabilities and SA completed with the capability to utilize the diminishing resources more optimally with decreased instances of collateral damage.

Further work related to creating a functional system based on the idea-phase description outlined in this paper needs to pay attention to operational security issues of using software and hardware in a digitized battlespace. Issues such as adequate level of constant energy flow and protection against violations caused by electronic warfare must be studied, tested and solved before the adoption of the system in any type of operational use.

The introduced idea-phase description of a communication system aims at being battle-proof from the perspective of using a swarms of UAVs in particular in that it guarantees the usability of the system functionality as the swarms of UAVs can automatically recreate a functional communication network and maintain an adequate distance between each UAV in all the circumstances and situations: once a UAV is destroyed or shot down, it has been programmed to destroy itself mechanically and electronically. The remaining fleets of UAVs corrects the formation of flying UAVs automated, to maintain a functioning and reliable communication system to ensure the communication system remains intact. SON supports the communication system formed by the swarms of UAVs together with SDRs. Unfortunately, when resources have been invested in further researching, developing, and, finally, implementing the system introduced here, the follow-up

papers cannot any longer be accessed in any public domain data sources.

REFERENCES

[1] K. A. Hempenius, A. R. Wilson, M. J. Kumar, N. Hosseini, M. E. Cordovez, and M. S. Sherriff, "A More Cost-Effective Unattended Ground Sensor Using Commercial Off-the-Shelf Products", Proc. of 2012 IEEE Systems and Information Engineering Design Symposium, pp. 62 – 67, ISBN: 978-1-4673-1286-8/12.

[2] R. A. Syed and R.S. Wexler, "Army Warfighter Information Network-Tactical (WIN-T) Theory of Operation", Military Communications Conference, MILCOM2013, 18–20 Nov. 2013, San Diego CA, pp. 1453 – 1461, doi: 10.1109/MILCOM.2013.246.

[3] S. L. Cotton and W.G. Scanlon, "Millimeter-Wave Soldier-to-Soldier Communications for Covert Battlefield Operations", IEEE Communications Magazine, pp.72 – 81, doi:10.1109/MCOM.2009.5273811, ISSN 0163-6804/09.

[4] T. Ulversøy, Software Defined Radio: "Challenges and Opportunities", IEEE Communications Surveys & Tutorials, Vol. 12, Issue: 4, Fourth Quarter 2010, pp. 531 – 550, doi:10.1109/SURV.2010.032910.00019.

[5] J. Mölsä, J. Karsikas, A. Kärkkäinen, R. Kettunen, and P. Huttunen, " Field test results and use scenarios for a WiMAX based Finnish broadband tactical backbone network" The 2010 Military Communications Conference, San Jose, CA, Oct. 31–Nov. 3, 2010, pp. 2014 – 2019. doi:10.1109/MILCOM.2010.5680446, ISSN 2155-7578.

[6] Scaldio, Reconfigurable Radio Transceiver IP, www2.imec.be/content/user/File/Brochures/GR2010_Leaflet Scaldio.pdf, accessed on 10th September 2014.

[7] C-Y. Chen, F-H. Tseng, K-D. Chang, H-C. Chao, and J-L. Chen, "Reconfigurable Software Defined Radio and Its Applications", Tamkang Journal of Science and Engineering, Vol. 13, No. 1, 2010, pp. 29 – 38.

[8] M. Islam, M.A. Hannan, S.A Samad, and A. Hussain, "Software Defined Radio for RFID Application", Proc. of the World Congress on Engineering and Computer Science 2009 Vol I WCECS 2009, October 20–22, 2009, San Francisco, USA, pp. 415 – 418, ISBN:978-988-17012-6-8.

[9] G. Thomas, "Situation Awareness Issues in Tactical Cognitive Radio", Proc. of 2012 IEEE International Multi-Diciplinary Conference on Cognitive Methods in Situational Awareness and Decision Support, 6–8 March 2012, pp. 287 – 293, ISBN 978-1-4673-0345-3/12.

[10] X. Dong, S. Wei, Y. Li, L. Wang, and L. Bai, "Service-Oriented Radio Architecture: A Novel M2M Network Architecture for Cognitive Radio Systems", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2012, Article ID 762953, 8 pages, http://dx.doi.org/10.1155/2012/762953.

[11] T. Saarelainen, "Modeling War as a Business Process with the Assistance of Service Oriented Architecture", ICDT 2014 The Ninth International Conference on Digital Communications, Feb. 23–27, 2014 Nice, France, pp. 1 – 7, ISSN: 2308-3964, ISBN: 978-1-61208-316-2.

[12] R. Adams, "Special Operations Forces Skills", Military Technology, Vol. XXXVIII, Issue 5/2014, p. 38 – 42, ISSN 0722-3226.

[13] T. Saarelainen and J. Jormakka, "Computer-Aided Warriors for Future Battlefields", The 9th European Conference on Information Warfare and Security ECIW2009, Lisbon, 6–7 July, 2009, Portugal, pp. 224 – 233, ISBN: 9781906638337.

[14] T. Saarelainen, "Improving the Performance of a Dismounted Future Force Warrior by Means of C$^4$I$^2$SR", Doctoral Dissertation, 212 pages, ISSN: 1796-4059, ISBN 978-951-25-2457-0, 2013.

[15] Y. Lin, H. Lee, M. Who, Y. Harel, S. Mahlke, and T. Mudge, "SODA: A Low-Power Architecture for Software Radio", Proc. of 33$^{rd}$ annual international Symposium on Computer Architecture, pp. 89 – 101, doi: 10.1109/ISCA.2006.37, 0-7695-2608-X,ISBN: 0-7695-2608-X.

[16] P. Pancholy, J. Kushwaha, and R. Chitranshi, "Smart 4G network:-Implementation of SDR & SON with Automatic EM Radiation control", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, November 2012, pp.14 – 18, ISSN:2319-5967.