This issue of AFDA News highlights some of the Finnish companies present at DSEI and at the Finnish - US Defence Industry Seminar in Washington D.C. in October. International markets and collaboration is increasingly important for the defence industry. With the economic austerity in the EU and the US, the defence companies are facing a challenging future. Competition in the political and fragmented markets becoming harder and harsher.

Finnish defence, aerospace and security industries answer these challenges by investing in R&D, developing the latest technology with the highest quality and finding the right partners. We, the Finnish companies, are focused experts from extreme conditions with a no-nonsense attitude.

Focused Experts

Finnland is one of the leading countries within innovation and this, of course, reflects to the defence industry as well. The Finnish defence, aerospace and security industries invest significantly in R&D and focus mostly on niche technologies. We deliver state-of-the-art solutions e.g. within C4, C4ISTAR, special structures and vehicles. Finland is the home for global market leaders in logistics, armored wheeled vehicles and turreted mortar systems.

From Extreme Conditions

Yes, Finland is a Northern and an Arctic country. The only country in the world, where all the harbors are covered with ice during the winter months (or would be, if we let that happen). And yet everything functions. But that’s not all. We have extensive expertise in the hot environments as well.

With extreme conditions I mean much more than solely a demanding climate. The size of the national economy in Finland sets a special condition for the companies to operate in. The national market is truly small and there is very little public funding for defence R&D. We have to be able to invent clever, efficient solutions which meet the customers’ need and budget. One of our competences is the ability to create premium products with long life-cycle performance as well as innovative and new methods of utilizing technology.

No-Nonsense Attitude

If you’ve ever met a Finn, you would know that we act more than we talk. We like to get straight to the point and focus on the outcome. And yes, we know of the jokes some nationalities have made about us doing just that. But we don’t even have a word for “small talk” in our language.

Action does speak louder than words in Finland. We deliver what we promise and strive for efficiency and perfection. This, in my belief, is one of the strengths of the Finnish defence, aerospace and security industries.

Enjoy reading this issue of AFDA News and see what these companies with their expert backgrounds and no-nonsense attitudes have to offer you!

Tuija Karanko
Secretary General
Association of Finnish Defence and Aerospace Industries
Market leader of modern 8x8 armoured wheeled vehicles

Patria is the undisputed market leader of modern 8x8 armoured wheeled vehicles with seven customer countries and contracts for nearly 1,400 vehicles. Core products are Patria AMV 8x8 armoured wheeled vehicle, related systems solutions and life cycle support services. Patria’s armoured wheeled vehicles feature the defence industry’s most advanced technology.

Patria has decades of experience and expertise in armoured wheeled vehicles and heavy weapon systems. The company works in close cooperation with customers and a broad international network of industry partners. Products and support functions are customised to each customer’s needs and meet NATO compatibility requirements.

A strong aviation expert and developer

Patria’s aviation expertise includes aircraft and helicopter assembly, composite structure manufacture, maintenance and modifications, and pilot training. Patria is one of the leading European providers of aviation life-cycle support services. An important competence area is the maintenance, repair and modification of the Finnish Air Force’s equipment. A history of over 90 years in the sector guarantees experience and commitment to the development of aviation.

System integration know-how

Today’s defence systems are large entities that are comprised of several subsystems. Patria’s solid system integration know-how ensures that the entire system functions faultlessly. Patria specialises in reconnaissance, surveillance, and command systems, as well as their integration and life-cycle support. Patria’s system integration know-how has been developed for decades to meet the needs of the increasingly complex systems used by customers.

Patria – unique products and customer-based solutions for modern defence

Patria is a defence, security and aerospace group whose products and services combine the best knowledge and expertise of the Group and its partners. Patria delivers its solutions to its strategic partner, the Finnish Defence Forces, and international market.
**Milectria Oy – From Plan to Solution**

Milectria is an expanding manufacturer of electrical systems.

Milectria invests in expertise and in the highest standard of work. The company is a flexible and responsive designer and manufacturer of electro-mechanical products for military industry.

Products are wire and cable harnesses, electrical panels and real estate centers. Milectria develops, designs and manufactures products for a variety of demanding operating conditions. The applications include specialized vehicles, communication systems, machine and equipment manufacture and hoisting equipment. Their success is based on specialization, expanded know-how, technology transfer and comprehensive service. Milectria has production in Finland, Estonia and Slovenia and employs 230 employees.

**Military Quick Stock**

Last winter Milectria launched a new service, Military Quick Stock. Through the Service it is possible to acquire either materials, or if needed, a ready-made assembled and tested cable harnesses. With the service customers will receive the products faster than before and equipped with competitive prices as well as quality guarantee. Military Quick Stock is based on a comprehensive stock. The wide range of components in stock ensures a smooth manufacturing process. This gives opportunity to sell special cables and components. The company has an online store, where products are displaced and orders can be made. Service is made easy to use and registration is not necessary.

**Traceability a crucial factor**

Milectria keeps detailed books of the production process and items used. Traceability is a crucial quality factor to the company and the customers. The importance of traceability is underlined in the demanding operating conditions. The traceability system includes a bar-code system that itemizes materials, work stages, work tools and employees. Traceability covers the product’s entire life-cycle. The itemization of our products is based on serial number method, which guarantees precise traceability. All the products are tested electrically before they are supplied to the customer. The material inventory allows Milectria to ensure excellent delivery times, from the first prototype to rapid serial production.

**Customer-specified products**

Most of Milectria products are customer-specified. Milectria delivers electrical systems for military and non-military purposes such as special vehicles, lifting devices and equipment and machine manufacturing. Typically the products are made in short series, including much manual work. The complicated solutions require a lot of know-how from the personnel. The company thinks it is important to participate in the planning process of cables at the earliest possible stage. That enables them to help the customer and together select correct materials, materials that are easy to get and are used in other projects. Milectria also provides the necessary documents and drawings for the project.
In a cyber world where most devices are linked to the worldwide web, everything is vulnerable. Security analyst Eeva Starck of Codenomicon, which provides software testing and network situation awareness solutions that protect national security, recommends a zero tolerance approach to hackers.

We live in a world where more and more devices are connected to the internet. This connectivity creates more attack vectors for hackers. Denial-of-service attacks can target any interconnected software that is not robust enough and, in a worst-case scenario, this can result in the installation of malware. Advanced persistent threats (APT) are all about zero-day vulnerabilities. An APT is a targeted attack upon which time and resources are spent. Particularly in attacks against critical infrastructure, hackers are persistent and will take time detecting vulnerabilities and building tailored attacks against them. Unfortunately, we are surrounded by vulnerable software.

Unknown, zero-day vulnerabilities are weaknesses in software just waiting to be found.

Get fuzzing
Known vulnerabilities, which have already been found and reported, are easily mitigated by installing security updates. Unknown, zero-day vulnerabilities are weaknesses in software just waiting to be found. Security updates, anti-virus software or firewalls cannot defend against them. If a malicious attacker targets an unknown vulnerability, reactive security measures are useless.

Discovering vulnerabilities within your software is essential to make it more robust. The only really effective way of doing that is through proactive security testing, also known as fuzzing. In short, fuzzing is simulating real-world attacks by sending malformed and unexpected messages (anomalies) to the software with the intention of disrupting services. When a given service eventually crashes, hangs or experiences degradation, an exploitable bug has been isolated.

Fuzzing can be deployed at any phase of the software development lifecycle, either in conjunction with other testing or during penetration testing before launching a critical service. The earlier these flaws are found, the cheaper it is to fix them. Easy-to-use commercial fuzzing tools let your engineers attack your systems with exactly the same techniques that hackers would use. With intelligent test automation tools, you will be the first to find zero-day vulnerabilities and can fix them before you become a target.

If there are no vulnerabilities that can be exploited, no malware can infect your systems. Robust infrastructures endure.

Network security is not just about robust software. It is also about knowing what is happening in your network. Situation awareness tools help control and fight network abuse. These tools are used by governments, critical infrastructure providers and other officials, such as CERTs, worldwide.

Organisations all over the world see abuse originating from their networks: attacks, scans, spam, botnet slaves and all types of active malware. It is impossible to catch these compromised hosts using network-based detection systems such as firewalls, intrusion detection or anti-virus systems. The amount of information that needs to be collected and handled can be overwhelming.

All companies are legally responsible for detecting and handling network abuse originating from their networks. Analysis and visualisation tools help find the incidents and the appropriate system administrators in order to take action.

Detecting the malicious traffic in a given network reveals malware, botnets and other possible abuse incidents. Situation awareness tools, such as Codenomicon’s Abuse Situation Awareness, are a set of detection, visualisation and analysis tools that plug into a wide range of data sources and render abuse handling fast and automated.

What’s happening inside your network?

Network security is not just about robust software. It is also about knowing what is happening in your network. Situation awareness tools help control and fight network abuse. These tools are used by governments, critical infrastructure providers and other officials, such as CERTs, worldwide.

Organisations all over the world see abuse originating from their networks: attacks, scans, spam, botnet slaves and all types of active malware. It is impossible to catch these compromised hosts using network-based detection systems such as firewalls, intrusion detection or anti-virus systems. The amount of information that needs to be collected and handled can be overwhelming.

All companies are legally responsible for detecting and handling network abuse originating from their networks. Analysis and visualisation tools help find the incidents and the appropriate system administrators in order to take action.

Detecting the malicious traffic in a given network reveals malware, botnets and other possible abuse incidents. Situation awareness tools, such as Codenomicon’s Abuse Situation Awareness, are a set of detection, visualisation and analysis tools that plug into a wide range of data sources and render abuse handling fast and automated.

This article has been published in Defence & Security Systems International, May 2012.
Elektrobit (EB) will exhibit its defense product portfolio at DSEI 2013 from 10-13 September in the Excel Convention Center, London, UK.

At DSEI EB is presenting EB Tactical Wireless IP Network - a system demonstrating a formation of wireless high data rate network connection. EB tactical Wireless IP Network is a high capacity backbone solution connecting mobile and stationary tactical units. The system is used to build Link, Point to Multipoint or MANET (mobile ad hoc network) connections in one logical network with automatic configuration.

**EB Tactical Wireless IP Network** smoothly connects to legacy communication infrastructures. Third party tactical data radios can be connected to the backbone through its gateway functionality. These radios can then utilize the high data rate IP (Internet Protocol) connection, as well as services like fixed network or satellite connection provided in another EB Tactical Wireless IP Network backbone node.

**EB is also presenting:**

- **EB Tough VoIP** product family providing tactical IP telephony in all environmental conditions
- **EB Soldier Terminal Platforms** for ruggedized handheld computers and smartphones
- **EB Wideband COMINT Sensor** for spectrum monitoring, recording, replaying, interception and analysis of wideband signals with remote operation
- **Intelligent Jamming Solutions** with EB Counter RCIED Platform as an example of intelligent and reactive jamming for the prevention of Radio Controlled Improvised Explosive Device (RCIED) threats

Please come and visit us at stand N5-446.

EB is actively looking for system integrators and distribution partners for its defense products. Learn more about our defense products at [www.elektrobit.com/defenseAuthorities](http://www.elektrobit.com/defenseAuthorities).

Elektrobit’s EB Tactical Wireless IP Network provides backbone connection between tactical data radio networks and fixed core networks.

Communication Solution Specialist

**Elektrobit (EB) demonstrates state of the art tactical communications technology at DSEI**
Survivability and threats
Survivability of a combat vessel in a hazard is a multifaceted problem. There will be questions like what is the floating position, and how the longitudinal strength, systems functionality and personnel are affected. How will the radar signature change and will the ship be salvageable? An important question is also how these various aspects interact together. Even if the actual situation never goes as modeled and everything happens too fast, it is good to have more than just an educated guess about the ship’s capabilities when it comes to survivability and mission completion. The current version of SURMA is capable of assessing damage from conventional warhead explosions in air (AIREX), either inside or outside a vessel, as well as global response with respect to underwater detonations (UNDEX). SURMA can be used to assess the effect of any changes on the survivability of a ship from all necessary aspects.

Why SURMA
When designing a naval ship for combat environment, various hazards and how they affect the ship, have to be taken into account. Traditionally, this means transferring lots of data, often in different file formats, between several computer models which calculate different aspects or phenomena, after every change made to the design. This is very time consuming, thus expensive, not to say frustrating. It is hard enough to get the results from different analysis to meet the requirements, and with the pressure from deadlines and budgets, this phase does not always get the desired attention. The result, unfortunately, can be a ship which is not as robust and combat resilient as intended to be. This is especially true when new innovative ship concepts and hull forms are introduced.

"SURMA can be used to assess the effect of any changes on the survivability of a ship from all necessary aspects."

Surma
– Your partner in naval combat survivability

Surma Ltd is a private Finnish company specialized in naval combat survivability. The mission of Surma is to provide efficient tools for comprehensive survivability assessment by naval designers. Surma also provides services for ship combat survivability assessment, calculations and research. The main product SURMA, Survivability Manager Application, is a software tool which integrates survivability assessment into the actual design process within a widely used commercial ship design platform, NAPA.

Survivability and threats
Survivability of a combat vessel in a hazard is a multifaceted problem. There will be questions like what is the floating position, and how the longitudinal strength, systems functionality and personnel are affected. How will the radar signature change and will the ship be salvageable? An important question is also how these various aspects interact together. Even if the actual situation never goes as modeled and everything happens too fast, it is good to have more than just an educated guess about the ship’s capabilities when it comes to survivability and mission completion. The current version of SURMA is capable of assessing damage from conventional warhead explosions in air (AIREX), either inside or outside a vessel, as well as global response with respect to underwater detonations (UNDEX).

Why SURMA
When designing a naval ship for combat environment, various hazards and how they affect the ship, have to be taken into account. Traditionally, this means transferring lots of data, often in different file formats, between several computer models which calculate different aspects or phenomena, after every change made to the design. This is very time consuming, thus expensive, not to say frustrating. It is hard enough to get the results from different analysis to meet the requirements, and with the pressure from deadlines and budgets, this phase does not always get the desired attention. The result, unfortunately, can be a ship which is not as robust and combat resilient as intended to be. This is especially true when new innovative ship concepts and hull forms are introduced.

"SURMA can be used to assess the effect of any changes on the survivability of a ship from all necessary aspects."

Surma Ltd is a private Finnish company specialized in naval combat survivability. The mission of Surma is to provide efficient tools for comprehensive survivability assessment by naval designers. Surma also provides services for ship combat survivability assessment, calculations and research. The main product SURMA, Survivability Manager Application, is a software tool which integrates survivability assessment into the actual design process within a widely used commercial ship design platform, NAPA.
varying positions with respect to these test structures. The results are then compared to simulations and used to enhance the accuracy of SURMA calculations. These thorough validation procedures have given a firm trust in SURMA assessments results.

What’s new in Surma

The next major step is to address the modeling of fire in a ship environment. Currently SURMA is linked to FDS (Fire Dynamics Simulator by NIST) including the Evac evacuation module. Another area of rapid development are the different signatures in the ship environment, e.g. radar cross section and especially underwater acoustic and magnetic signatures. Surma-team will be considerably strengthened in this field in the imminent future.

Even though this article has discussed the usage of SURMA in naval vessel design, this approach is applicable with negligible modifications to any ship design process as well as offshore platforms, where fire and explosions are also real threats.

There is also a change in the executive board of Surma. Mr. Martti Helamaa, a specialist in electro-magnetics, is appointed as the new CEO, starting in September. For the last two years he has been the General Manager of Surma Inc, our subsidiary in United States. Mr. Kristian Torniainen, who has lead Surma since its foundation in 2007, will be concentrating on marketing, sales and customer relations. The dynamic and innovative Surma-team continues developing to serve better its ever increasing network of partners and customers.
The antenna is a crucial element of the RF system, because it converts the radio amplifier’s power to electromagnetic waves. To achieve the best possible transmission over a wide bandwidth, it would require that the antenna is ideally in tune over the entire used frequency range. Naturally an antenna is, however, in tune only in a narrow band and therefore the matching of a wide-band antenna is challenging. In order to obtain an adequate VSWR (Voltage Standing Wave Ratio) level inductive or resistive components are often needed in the matching network. It means that trade-offs in performance have to be made.

COJOT has developed an active band switching technology for wide-band antennas that allows optimizing the matching more efficiently across a wide frequency range. This technology improves the antenna’s overall performance and provides additional benefits for enhanced efficiency. In this approach the entire frequency range is split into smaller portions. A similar method is already utilized in modern communications within the HF bands. With modern VHF and UHF tactical radio waveforms modulation techniques are more challenging than in HF bands. They commonly include techniques called frequency hopping, where the signal is rapidly switching among various frequency bands. The time to make the switch from one band to another is significantly shorter than the time which is required by HF devices.

The Principle of Active Matching

Matching problems occur when a broadband antenna needs to be matched to 50 Ohm impedance, with low enough VSWR levels throughout the whole operating bandwidth.

Traditionally the matching of such a wideband antenna is done with inductive or resistive components that are accompanied by considerable mismatching losses. The red line in Figure 1 presents the matching of this VHF radiator without matching components. When the antenna is in tune the mismatching loss is small and additional matching wouldn’t be required. Those areas are however rather narrow compared to the entire frequency band this antenna is supposed to work in. The blue line shows the typical mismatching loss of a wideband antenna that is matched with passive components. The maximum VSWR level is set to 1:3, which is quite a typical requirement in communication applications. It can be seen that wideband matching is generating some 5 dB loss to the whole frequency band. The antenna’s overall performance is significantly affected, as the areas where the antenna is naturally in tune can’t be fully exploited. This shortage can be avoided through antennas that use tunable matching.

The basic idea of active band switching is to split the frequency band into smaller slots and match each of these slots separately. Thus the areas where the antenna is naturally in tune can be fully obtained and the antenna’s performance is improved.

Figure 2 represents the simplified block diagram of tunable matching. Benefits

Wideband antennas with active matching overcome some shortcomings of traditional passive matching methods. Active band switching improves remarkably the antenna’s overall performance e.g. to provide a better coverage and extended communication range. It allows considering the additional useful opportunities that this technology offers, i.e. its potential to considerably reduce power consumption and its capability to achieve with a smaller sized radiator a performance, which is similar to that of a longer, passively matched radiator. Higher out-of-band interference rejection as the antenna is operating at only a small area of the complete frequency range at this time provides better signal to noise ratio to the radio system.

COJOT presents and demonstrates the new TA30512M, active band switching wideband VHF/UHF antenna at DSE I 2013.

For more information see www.cojot.com.
Robonic highlights its versatile UAV launchers for the U.S. market

Safran group company Robonic used its presence at this month’s AUVSI Unmanned Systems 2013 event in Washington, D.C. to focus on applications for its high pressure pneumatic unmanned aerial vehicle (UAV) launchers in the United States.

“His is where the largest market is,” says Robonic Managing Director (CEO) Juha Mosisio about the U.S. “We are working closely with some of the U.S.-based UAV systems integrators and we believe this market presents a great opportunity.”

The Finland-based company, which is a subsidiary of the Safran group’s Sagem business unit, produces the versatile KONTIO UAV launcher, and is developing a smaller variant – OHTO – which meets the United States tactical UAV market’s present requirements. Both launchers’ names are drawn from the approximately 100 words in the Finnish language for “bear.”

With its adapter package designed to meet the diverse requirements of many UAVs and target drones, KONTIO can launch over 20 types of the world’s unmanned aerial vehicles, both tactical and target, and is capable of launching a 250 kg vehicle at 55 m/s off the end of the ramp or a 160 kg air vehicle at 70 m/s. Mosisio says because of the launcher’s design, rapid deployment capability, unique launch lock mechanism and the possibility to integrate varying adapter packages – which meet the individual characteristics of different vehicles – this launcher suits all small and tactical UAVs currently in the U.S. inventory.

The smaller OHTO version, which the company is now developing, will have approximately 60 percent of the KONTIO’s power, and provide coverage for the smaller- and mid-sized UAV market as well as a limited target market.

Currently, Robonic launchers support the RUAG Aviation Ranger in use in Finland, the Sagem Sperwer family of UAVs, the Lockheed Martin Fury, as well as a variety of aerial targets ranging from Meggitt’s Vindicator and Banshee to the Cassidian DT-family of targets and most recently CEi’s (a Kratos company) Firejet.

We are working closely with some of the U.S.-based UAV systems integrators and we believe this market presents a great opportunity.
Lockheed Martin Fury ready for launch on a Robonic Kontio launcher.