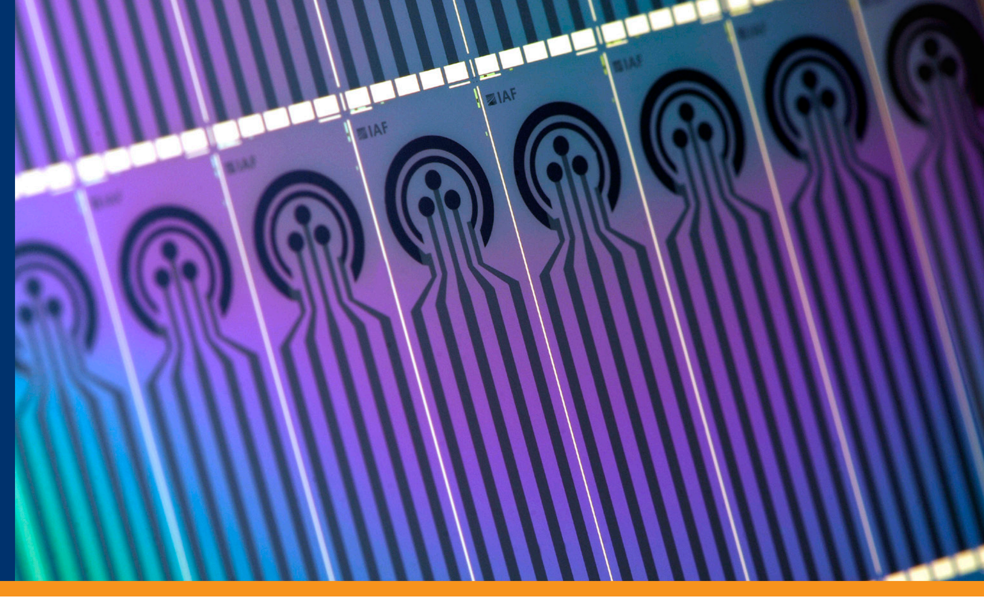
Fraunhofer VVS

FRAUNHOFER GROUP FOR DEFENSE AND SECURITY VVS

GRAND DEFENSE-TECHNOLOGICAL CHALLENGES FOR EUROPE POST-2020

POSITION PAPER

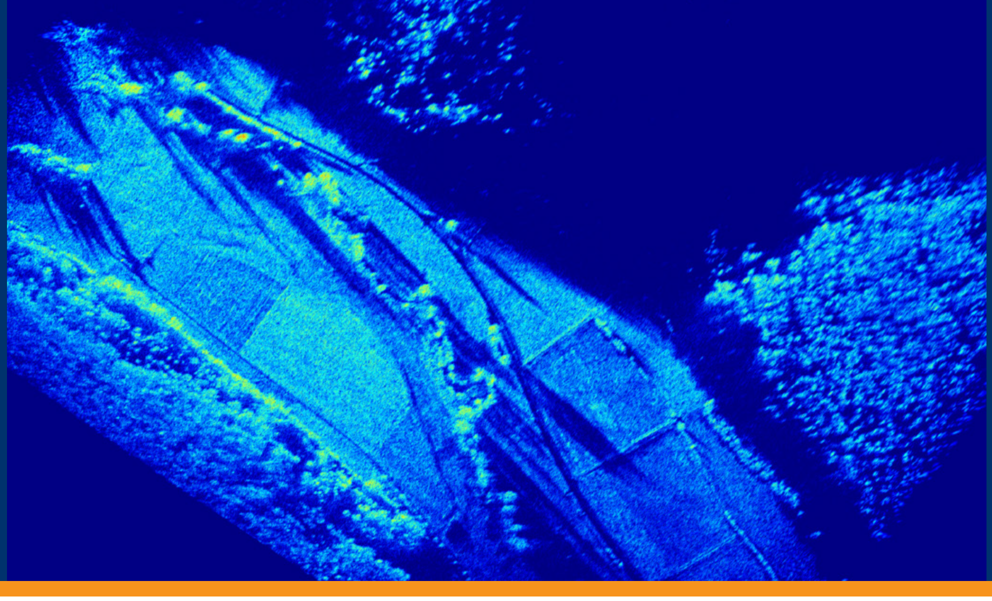
© Fraunhofer ICT



© Fraunhofer IAF

Index

© Fraunhofer FHR



© Fraunhofer FKIE

1 Introduction

Defense cooperation at EU level is deepening with increasing pace. The current momentum was initiated both by the EU-Commission with its Communication »Towards a more competitive and efficient Defence and Security Sector«- COM(2013) 542 – and the »European Council Conclusions on Defence« - EUCO 217/13 – in 2013, and further fuelled and concretised through documents such as the EU's Global Strategy for its Foreign and Security Policy and its related »Implementation Plan on Security and Defence«, as well as the »Commission's European Defence Action Plan« (EDAP) - COM(2016) 950 - from 2016, and the launching of the »European Defence Fund« - COM(2017) 295 – with its Research and Capability Windows. Intergovernmentally, the next step reached was the Council of the EU Decision establishing Permanent Structured Cooperation (PESCO) in December 2017, with 25 EU Member States participating (Denmark, UK and Malta opted out), which could be incentivised by the »European Defence Fund«.

As far as **defense research** is concerned, with the start of the »Preparatory Action on Defence Research (PADR)« in 2017 the first programmatic step towards a common defence research programme for the first time ever on EU level, known as the supposed »EU Defence Research Programme (EDRP)« post-2020, was successfully implemented. Given the fact that these EU activities should complement (thematically as well as budget-wise) defense research conducted on EU Member State level (including bi- and multilateral R&T cooperation), the question is raised which research themes could or should be addressed by the EDRP post-2020. Following the logic of the »European Defence Fund«, there are two connected main political goals to be achieved by these activities – enhancing the **EU's strategic autonomy** by developing strategic military capabilities and required key technologies in critical areas (Critical Defence Technologies, CDTs), and strengthening the **technological leadership of EU defense industry**. Typical for defense research, a combined top-down (capability pull) and bottom-up (technology push) programme planning approach for the EDRP seems to be most suitable, with the military capability requirements and priorities being identified and agreed (with the support of EDA) by the EU Member States at EU level, as well as the R&T priorities. The top-down approach currently is on its way through the ongoing 2017/18 revision of EDA's Capability Development Plan (CDP), expected to provide a new set of capability priorities specifying and complementing the priorities highlighted in the EU Global Strategy, the »Implementation Plan on Security and Defence« as well as the »European Defence Action Plan«. At the same time, the stakeholders of the »European Defence Industrial and Technological Base (EDTIB)« driving the technology push in defense in the EU, including the European Research and Technology Organisations (RTOs) such as Fraunhofer, are expected to provide perspectives, insights and guidance for decision makers on the most relevant technological challenges and fields that are likely to determine strategic autonomy and technological leadership in defense post-2020.

Inspired by the »grand societal challenges for Europe« as defined and specified in the EU's Horizon 2020 research programme, the Fraunhofer Group for Defense and Security (VVS) proposes to commonly identify »grand defense-technological challenges post 2020« across the EU that currently are assumed as being already or becoming major drivers for strategic autonomy and technological leadership in the foreseeable future, from the technological point of view. Thus, **seven Grand Defense-Technological Challenges for Europe post-2020 (GCs)** as suggested by Fraunhofer VVS are outlined as follows; these GCs should be addressed and further specified with priority in the EDRP.

An **eighth area** of equal importance but a different kind of challenge has been identified and sketched too, but because of its different programmatic nature it is not included in the list of the seven GCs: it concerns the need for **European Autonomy for Critical Components and Scientific Software Tools for Defense Applications**. More and more, EU Member States' access to critical components is limited by export control regulations (like ITAR, the US International Traffic in Arms Regulations). Even scientific software tools for defense applications are not shared among transatlantic partners and partly only out-dated versions are accessible by European nations. The idea of **European Defense Autonomy** is to become independent with respect to **critical components** as well as with regard to the scientific evaluation of approaches and design solutions for defense applications. Examples are **high-acceleration sensors** or **chemical simulation codes** for the performance of energetic materials, **underwater detonation codes**, or **codes including big data methods**. Therefore, European research and innovation activities on such critical defense technologies should be intensified to ensure own up-to-date applications and foster future innovations, and to ensure the EU's strategic autonomy in this regard.

© Fraunhofer FKIE

2 Grand Defense-Technological Challenges

The following is a list of the Grand Defense-Technological Challenges for Europe post-2020 from the point of view of Fraunhofer VVS. As mentioned before, these challenges should be further developed and specified to extract concrete research topics. Research activities addressing these challenges need to include investigations into their ethical, legal and societal implications (ELSI), as it is furthermore proposed to also consider including ELSI in defense as a dedicated accompanying research subprogramme throughout the EDRP.

2.1 Artificial Intelligence and Autonomy

Artificial intelligence (AI) and autonomous systems are expected to become crucial military force enablers in the mid-2020s. Collectively, AI encompasses several technologies that aim to mimic the human cognitive processes in technical systems, either partly (soft AI) or completely (hard AI). **Deep (machine**) **learning and natural-language processing (NLP)** are among the current technological developments to enable AI, whose functionality in turn is an essential requirement to enable **cognitive technological systems**. AI is expected to significantly improve a number of military capabilities, such as military ISR (Intelligence, Surveillance, Reconnaissance) through smart exploitation of vast heterogeneous sensor data, supported by **big data analytics**, intelligent information retrieval in military data lakes and **automated decision support**, autonomous cyber defense systems, automatic language translation for soldiers etc. Moreover, AI will also be a major driver in creating fully autonomous unmanned systems. In complex battlefield environments, **automated/autonomous unmanned systems** are likely to become superior to human-piloted systems in the near future, calling for technologies that facilitate **natural user-system interaction** (e.g. speech, gestures), enable intuitive manned-unmanned teaming (e.g. **human-machine/-robotic/-swarm interfaces**) and achieve **efficient resource management and mission execution of large-scale distributed systems, multi-robot systems or UxV swarms**. Research on **interoperable solutions** on a European level also is essential for the aspect of **survivability of European forces** and **counter-measures** against adversarial usage of AI-augmented systems.

© Fraunhofer IAF

Topics could include (but are not limited to):

- Resource management for optimal usage of sensors, communication networks and platforms in accordance with the swarm mission,
- Adaptive motion behaviors for unmanned ground systems taking tactical requirements and procedures into account,
- Intuitive routine interaction among soldiers and UxVs in teaming missions,
- Intelligent C2 support for large-scale distributed systems taking the system's state and capabilities as well as the mission's objectives and status into account (e.g. mission compliant task assignment to individual systems),
- Big data analytics and AI methods for
  - o Fake News Recognition,
  - o Social Media Analysis for OSINT,
- AI and deep learning for cognitive radio frequency applications (Radar/Communication/EW),
- Ensure European forces' future capacity to act: Review of existing survivability solutions specifically in the context of AI and autonomy, enhancement of their technological capabilities to allow European forces to sustain and complete their mission successfully when technologies enabling AI and autonomy are used by opposing forces. Development of resilient systems.

© Fraunhofer IIS

2.2 Digital Battlefield

As in civil society, the digitization of military forces is expected to significantly increase in the upcoming years. This trend calls for a number of communication technologies enabling digital networked forces, ranging from IP-based sensors and actuators in all kinds of military systems (**internet of battle things**), **software defined radio, mobile ad-hoc communication networks** and **software-defined networking** to **smart logistics**. **Artificial intelligence** in concert with **big data analytics** (e.g. in the form of battlefield management systems) will be essential to process and interpret the flood of digital data. New human-computer interfaces like **augmented and virtual reality** will be used to present this curated data to the end user. Furthermore, there is a need for solutions to retain full use of the electromagnetic spectrum even in contested environments to ensure the operational capability of own, digitized forces (EM spectrum dominance). Here, **electronic/cyber protection and counter measures** will be of utmost importance.

Topics could include (but are not limited to):

- Increasing the spectral efficiency by EM monitoring with AI for SIGINT in tactical scenarios, by cognitive radio and software defined radio technologies including modern networking waveforms,
- Harmonization and standardization of architectures (like software communications architecture, SCA, or European secure software radio, ESSOR) and cross-layer interfaces (like dynamic link exchange protocol, DLEP),
- Advanced sensor data fusion for heterogeneous, distributed sensors in the digital battlefield,
- Advanced tactical situation display (sandbox) applying different technologies of Virtual Reality for distributed mission planning and military decision making,
- Augmented Reality (AR) for supporting and increasing situational awareness of dismounted task forces at urban operations. AR supporting a correct understanding of the tactical situation (blue, red, yellow forces) and awareness of dangerous areas (e.g. contaminated areas, mine fields, snipers),

© Fraunhofer FKIE

- Mission preparation and mission support by means of Augmented Reality as advanced situation analysis and planning tool,
- Deep (machine) learning and natural-language processing (NLP) based speech recognition for Smart C2 Systems,
- Automated Vulnerability Detection in soft- and firmware based on AI and automated patching of vulnerable systems,
- Kill-Chain-Detection based on Big Data and AI to detect cyber-attacks.

2.3 Quantum Technologies for Defense Applications

Rapid developments in quantum technologies – specifically **quantum sensors, quantum imaging, quantum communications and quantum computers** – will have a tremendous impact on defense and security applications. **Quantum sensors** could, for instance, be used in the future to detect very small magnetic fields at room temperature with ultra-high spatial resolution and very high sensitivity.
Realized by nitrogen defect centres in monocrystalline diamonds those sensors will have numerous defense applications like **GPS-independent navigation** or the detection of very small magnetic field anomalies. **Quantum communications** can, for example, be used to **secure communications** by exchanging cryptographic keys employing quantum physical phenomena. If **quantum computers** are realized in the future, then they will be able to break several important cryptographic schemes that are widely used today. In addition, quantum computers could be used to design novel materials from the atom up and might speed up some artificial intelligence applications like classification.

© Fraunhofer FHR

© Fraunhofer IAF

2.4 Advanced Radar Technologies

Using radio frequencies and millimetre waves is essential for communication, situation awareness and fighting targets. Emerging technologies are expected to improve these abilities significantly: Novel **wide-bandgap materials** enable new device concepts for radar applications or high-bit-rate wireless communication (up to 1 Tbit/s). **Multi-functional coherent radar networks (MFCRN)** will lead to an increased detection capability (sensitivity and range) and thus an improved situational awareness. In combination with cutting-edge **radar-antenna** and **RF designs**, these networks will even be able to detect hypersonic missiles with low radar cross section reliably. New dimensions of operating the electromagnetic regime can be opened as well: Radar applications and RF-communication (civil as well as military) use the same, heavily crowded electromagnetic spectrum. The approach of **radar-communication co-design** will make the usage of limited bandwidth more efficient with the military advantages of greatly expanded coverage, cost saving on infrastructure, efficient spectrum usage, adaptive signal design and tailored illumination. These advanced radar technologies contribute to the GCs »Digital Battlefield» and »Future Weapons« in providing enhanced situational awareness.

Topics could include (but are not limited to):

- Heterogeneous integration of III-V compound semiconductors with silicon CMOS,
- Multiple input, multiple output (MIMO) radar concepts,
- Antenna technology and metamaterials for multi-functional radars,
- Advanced electromagnetic modelling for low-observable targets,
- 3D printing of high frequency structures for new antenna concepts,
- Heterogenic integration of SiGe and InP/GaAs for systems concepts above 100 GHz (system in a package),
- Time synchronisation of spatially distributed radar sensors.

2.5 Power Supply and Efficiency

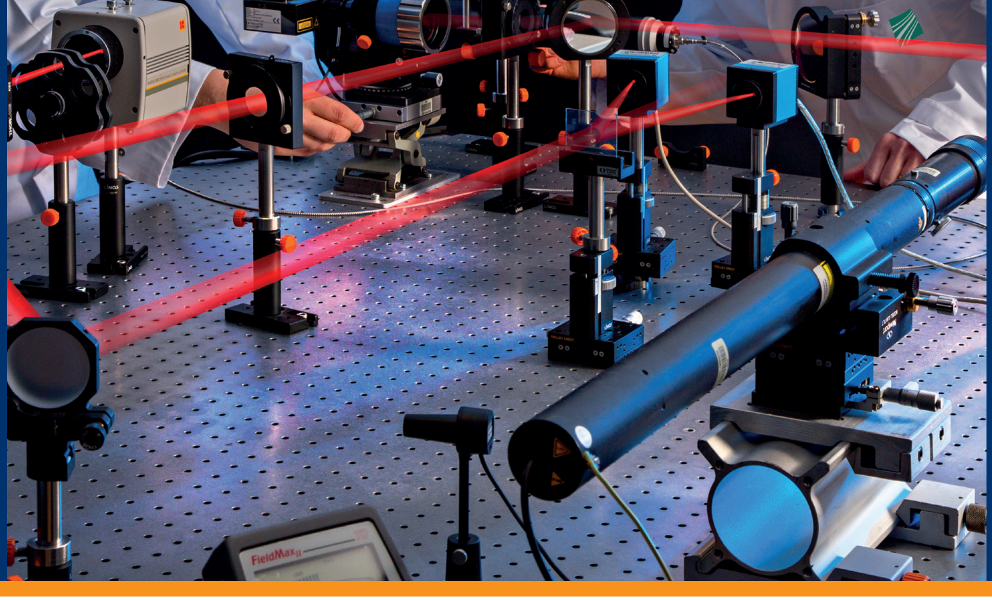
Energy is fundamental to military operations, enabling movement, speed and endurance and dictating deployment time and range for air, land and sea forces. A guaranteed, easy and logistically simple power supply designed for military requirements is prerequisite. More **efficient energy use** is needed to cope with the increasing energy demands of modern warfare. Taking into account the variety of energy converters used across different platforms, the required fuel and working energy must be defined as simple as possible – preferably **one fuel** and **one working energy**. Ideally, because of logistic reasons, the basic fuel should be **synthetically produced** with **less impurities** and **higher energy densities**. This vision could only be realized in a coordinated European approach as it is paramount to ensure interoperability. **Electricity** is the working energy of the future, the major challenge in this field is **high density/high power storage** and **electrical power conversion**. **Renewable energy opportunities** should be used for contingency bases to minimize the burden of resupplying operational forces with liquid fuel. **Energy-harvesting** technologies that collect energy from the environment to power small electronic devices like sensors can also reduce the need for resupply.

Topics could include (but are not limited to):

- Compact, efficient and robust power converters for a wide range of power levels.

2.6 Next-Generation Effectors

There are numerous concepts for next-generation weapon systems, promising new or at least enhanced and scalable capabilities beyond those of todays employed systems. One of the most prominent technologies in this respect are **high-energy laser weapons**, which can be operated with very low cost per shot, high precision and agility in a large variety of defense applications, ranging from dazzling or destroying sensors of hostile UAV to the hard-kill of incoming missiles or mortar rounds. Another example for directed-energy weapons are **high-power electromagnetic (HPEM) effectors**, which can be deployed to jam or destroy at distance many kinds of



© Fraunhofer IOSB

electronic equipment without being lethal to humans. Generally, casualty aversion is the driving factor in the shift to **non-lethal weapons (NLW)** which constitute a large variety of electromagnetic, kinetic, mechanical, acoustic and non-lethal chemical devices that can be used to reach operational goals with minimal damage to non-combatants, combatants and the environment. **Electromagnetic railguns** are weapons using electric energy to fire inert or explosive projectiles, offering enhanced muzzle-velocity and thus enhanced range or higher impact velocity. Recently, there is a revived interest in the development of **hypersonic missiles**, which offer greater engagement ranges with possibly higher hit rates for guided missiles, as well as shorter flight times, assured penetration of missile-defense systems and enhanced effectiveness against bunkers or hardened targets. An important underlying technology for ammunitions and weapon systems are next generation **energetic materials** with enhanced performance, adjustable effects against specific types of targets, long-term stability as well as reduced sensitivity and vulnerability. In addition, effective engagement capabilities in the cyber domain enabled through **offensive cyber and information operations** will be paramount for military forces in the digital age.

Topics could include (but are not limited to):

- Air-Based Laser for Defence: scalable high-energy laser weapon, small, powerful and efficient enough to be used in air-based platforms. Enabling the use of laser-based effectors in various defense systems e.g. for laser protective shields,
- New fuse technologies for next generation effectors,
- New protective solutions against new effectors & protection of infrastructure: new materials, new methods for modelling and simulating advanced, functional materials, new ways of production (additive manufacturing), and creating resilient systems/infrastructure.

2.7 Human Performance Enhancement

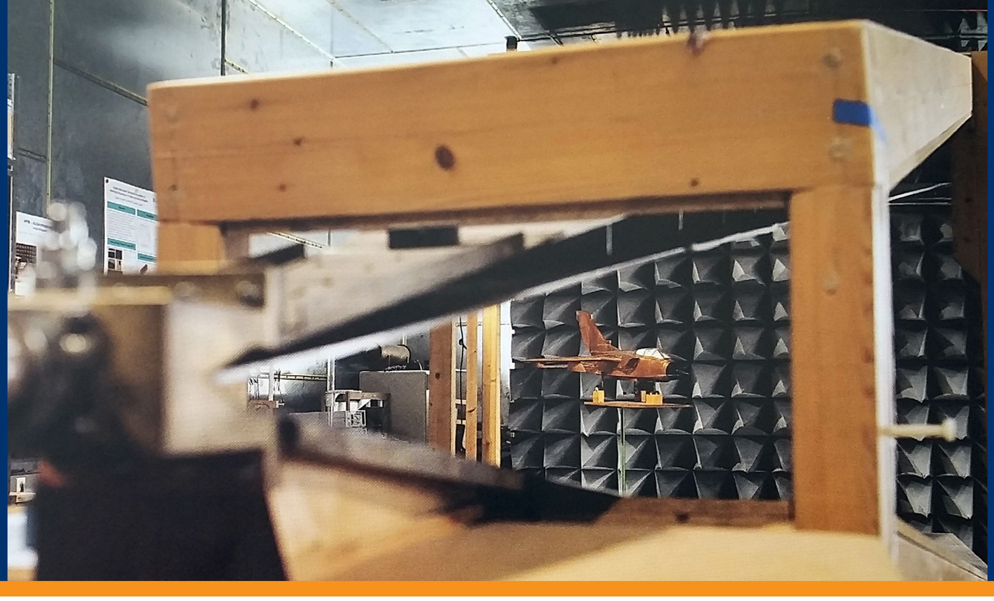
As military systems become increasingly sophisticated and capable, human operators must keep pace with the technological developments. Human Performance Enhance-

© Fraunhofer IOSB

ment (HPE) is thus poised to become another grand challenge in defense, driven by scientific breakthroughs and technological innovations in life science (e.g. CRISPR) as well as by a trans-societal desire for self-optimization. Already, there is a huge spectrum of approaches to enhance physical and mental abilities, ranging from **dietary supplements, pharmacological substances, augmented reality** applications and **exoskeletons** to **transcranial stimulation** protocols, **brain-computer interfaces** or even **genetic modifications**. Moreover, in the future, **smart textiles, e-skin, wearables, ingestibles** and **embeddables** will also provide detailed physiological and mental state measures for the individual soldier (»**quantified soldier**«).
With respect to the digital battlefield (see section 2.2), fusion of this information with other data streams will unlock valuable command and control capabilities (**continuous health monitoring, medical decision support** etc.).

Topics could include (but are not limited to):

- Application of wearables for measuring biological and physiological workload of soldiers (biomonitoring),
- Big data methods for processing biomonitoring data for soldier performance assessment for optimizing mission performance,
- Implementation of Augmented Reality to enhance soldier performance and cognition by means of a realistic and consistent integration of additional information into the soldier's sight,
- Assessment of physiological assisting systems for enhancing soldier performance in terms of endurance and maximum force (an »Exoskeleton»). This topic refers to the identification of relevant needs for enhancement and possible solutions for this.



3 Editorial Notes

Editors

Prof. Dr.-Ing. Jürgen Beyerer
Group Chairman
Fraunhofer Group for Defense and Security VVS

Prof. Dr. Peter Martini
Deputy Group Chairman
Fraunhofer Group for Defense and Security VVS

Editorial Team

Fraunhofer Institute for Technological Trend Analysis INT,
Business Unit Defence Technology Foresight

Contributors

- Fraunhofer Institute for Applied Solid State Physics, IAF
- Fraunhofer Institute for Chemical Technology, ICT
- Fraunhofer Institute for High Frequency Physics and Radar Techniques, FHR
- Fraunhofer Institute for Communication, Information Processing and Ergonomics, FKIE
- Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institute, EMI
- Fraunhofer Institute for Technological Trend Analysis, INT
- Fraunhofer Institute of Optronics, System Technologies and Image Exploitation, IOSB

© Fraunhofer EMI

GRAND DEFENCE-TECHNOLOGICAL CHALLENGES FOR EUROPE POST-2020

POSITION PAPER

Chairman of the Group
Prof. Dr.-Ing. Jürgen Beyerer
Fraunhofer IOSB
Fraunhoferstrasse 1
76131 Karlsruhe, Germany
juergen.beyerer@iosb.fraunhofer.de

Deputy Chairman
Prof. Dr. Peter Martini
Fraunhofer FKIE
Fraunhoferstrasse 20
53343 Wachtberg, Germany
peter.martini@fkie.fraunhofer.de

Managing Director
Caroline Schweitzer
Fraunhofer IOSB
Gutleuthausstrasse 1
76275 Ettlingen, Germany
caroline.schweitzer@iosb.fraunhofer.de

www.vvs.fraunhofer.de