Titel: Free Play of Innovative Forces or Systematic Restructuring?

Digital technologies will play a key role in the transformation of critical infrastructures, for example the power supply, which are essential for the location, for our prosperity and for our society’s performance. However, digital transformation must not put the reliability of supply systems at risk. So, what are the requirements of a reliable energy and transport infrastructure? The use of disruptive technologies challenges infrastructure operators as well as the economy to jointly implement effective measures, such as innovation partnerships, promptly.

Chair: DI Theresia Vogel
Director Climate and Energy Fund, Vienna

Coordination: Mag. Katja Hoyer
Public Relations Manager, Climate and Energy Fund, Vienna

01:15 p.m. – 01:25 p.m. Welcome
Markus Mooslechner (moderator), Executive Producer, Factual Entertainment and Format Development Terra Mater, Vienna

01:25 p.m. - 01:45 p.m. Opening remarks
Theresia Vogel, Director Klima- und Energiefonds, Vienna
NN, Ministry for Transport, Innovation & Technology, Vienna

01:45 p.m. – 02:15 p.m. Keynote
Marc Elsberg, Bestselling author of “Blackout”, Vienna

02:15 p.m. - 02:30 p.m. Interaction of podium and plenum

02:30 p.m. - 02:50 p.m. Statement and Discussion
Bernd Klöckl, Head of Grid Planning, TenneT TSO GmbH, Bayreuth

02:50 p.m. - 03:10 p.m. Statement and Discussion
Martin Schaffer, Global Head of Secure Products & Systems SGS Digital Trust Services GmbH, Graz

03:10 p.m. - 03:30 p.m. Interaction plenum

03:30 p.m. – 03:45 p.m. Coffee Break

03:45 p.m. - 04:05 p.m. Statement and Discussion
Marta Molinas, Professor at the Department of Engineering Cybernetics, Norwegian University of Science and Technology, Trondheim

04:05 p.m. - 04:25 p.m. Statement and Discussion
David Carvalho, Founder & CEO of NAORIS, London

04:25 p.m. - 04:45 p.m. Statement and Discussion
Bernd Datler, Director ASFINAG Maut Service GmbH, Vienna

04:45 p.m. - 05:30 p.m. Interaction plenum and summary of key findings

05:30 p.m. – 06:00 p.m. Demo live-hacking of a critical infrastructure (David Carvalho)
Marc Elsberg, Bestselling Author and Pioneering Thinker, Vienna, Austria

Abstract
In his thriller „Blackout“, Marc Elsberg tells the story of a fundamental change, which has taken place within our society during the past decades - unnoticed by most of us. Never before in the history of mankind have so many people lived so comfortably, healthy, long and secure as today. But this lifestyle comes at a price. Never before in the history of mankind so many people have been dependent on the smooth functioning of highly developed, precisely coordinated and mutually interdependent structures and technologies. One of the most important of those sub-systems in this global system of systems is power supply. How fundamental this change has been, becomes obvious once those systems vanish, break down or no longer work. Using different examples from all parts of our daily lives – from food and water supply or health services to money supply – Marc Elsberg exemplifies the importance of those systems to our lifestyle, but also our modern society’s vulnerability.

What – as one example - does it mean for an outsourcing-just-in-time-society and its supply chains if basically all gas stations seize to work? Be it in industrial production, industrialized agriculture or modern hospitals, which get provided with thousands of portions of pre-packed food three times a day by an external contractor? Developments like the coming “Internet of everything and everyone” will only increase exponentially those mutual interdependencies and complexity of our social fabric.

Those and other examples will show, how nowadays all stakeholders need to look much further beyond their own nose than we used to do.
Bernd Klöckl, Head of Grid Planning, TenneT TSO GmbH, Bayreuth, Germany

Abstract
The Electrical Power Systems in industrialised regions like Europe are highly interlinked, extremely complex and large machines that are being operated based on the engineering experience of many decades. Their operating principles have been designed to ensure a maximum of stability and resilience against all kinds of threats, be it from internal system faults, be it from external disturbances by natural disasters or man-made threats.
Currently there are two main developments that create increased complexity, but also additional chances and increased flexibility, which are
- a more volatile system operation because of the energy transition, and
- innovation activities driven by society’s digitalisation.
Research, development and innovation activities for the future system operation now require attention to maintain the high level of security of supply also under these changing boundary conditions.
This contribution to the discussion will differentiate between possible system threats and show how the system layout respects outages and faults. On the other hand side, the high chances offered by new digital technologies for stable system operation and security of supply are described.
Abstract

The world is becoming increasingly convenient thanks to the Internet of Things (IoT). Contactless payments, home automation, autonomous driving and smart factories are just a few examples. New mobile communication standards (e.g. 5G) allow faster interaction between devices, which enables new use cases, such as smart cities, smart factories or autonomous driving.

IoT solutions are flooding our markets with very few restrictions when it comes to IT security. Currently, almost no regulation or legislation is in place which addresses this issue appropriately. The challenge here is complex, as security cannot be dealt with at one single stage: systems need to be designed securely and remain resistant against attacks throughout their life-cycles. This means devices need to be updatable to be able to respond to new developments and forms of attack. This in turn requires the availability of backend systems offering corresponding services and secured communication channels between devices and the backend. And even if it is possible to provide secure solutions, how can we be sure that they are properly implemented, configured, deployed and operated? How can we detect cheaters in the supply chain?

One way to stop unsecure products entering the market is to implement corresponding legislation, standards and conformity assessment, as in other areas which impact on our day-to-day lives. Cars need to pass crash tests, new types of drugs need to be approved, children’s toys are subject to safety checks, and electrical systems must undergo conformity tests – the list goes on.

As a first step into that direction, the EU Cybersecurity Act has been formally published on June 7th as Regulation (EU) 2019/881 and came into force on 27th of June 2019. It sets a top-level framework for European Cybersecurity Certification as a first step. Still there is quite a way to go because attacks are evolving quickly, and the current security certification landscape is not ready to cope with this in a holistic way. The criteria for conventional conformity assessment are quite static. Physical laws do not change, i.e. a day after a certificate has been released, repeating the test usually results in the same outcome. This is not the case when it comes to cybersecurity. The forms of attack are changing all the time. What is state-of-the-art today may no longer be tomorrow. Conformity assessment therefore needs to undergo a revolution in response to these new shifting circumstances. Soon, everything will need to be continuously checked for resistance against attacks, in ways which are efficient in terms of time and costs.

Another challenge is to ensure that components that have been assessed by independent third parties are finally really ending up in the intendet solutions in the field, as currently being discussed quite broadly on EU-level for the roll-out of 5G equipment. There is a risk of getting exposed by backdoors built into networks, but also end nodes in factories, at home or in the car. Backdoors can be used for espionage, but also to break the integrity of systems or even shutting them completely down. For example, a secret kill-switch built into all HW chips of the telecom network could potentially enable a hacker to shut down the entire digital world of a country and beyond.
Marta Molinas, Professor, Department of Engineering Cybernetics, Norwegian University of Science and Technology, Trondheim, Norway

Abstract
In the transition towards an energy system that is sustainable, the smart home is one of the latest emerging ideas in relation to the application of information and communication technologies (ICT) in the home. The introduction of smart home technologies may have the potential of creating entirely new practices and normalizing new expectations to comfort, convenience, entertainment, security, health care and so on. Although smart functions may be applied to achieve energy savings, they are also open to accommodate other concerns, which may have negative consequences for total energy consumption. This talk will take the thoughts of the audience not on the energy issue itself but on how to efficiently capitalize on the combination of human brain capability and ICT functionalities. The central idea is to bypass manual or remote control of devices in the digitization of the homes and surroundings by creating a direct path of communication between the brain and the appliances in the home. Internet connectivity and ICTs combined with sensor technologies open new opportunities for taking care of the elderly and in general people with physical disabilities, for instance, brain-managed remote control opening and closing windows and doors, drawing curtains, riding wheelchairs, turning lights and music centers on and off and lifting and lowering kitchen tables. As the trend of ICT will continue to grow, application of AI and machine learning techniques will be essential to this realization. Not only for the interconnection of the IoT in the smart home but of the internet of Things and Brains (IoT-B). This transformational thought will bring fresh ideas to the table, such as the prospects of Telemedicine enabling direct communication of recordings from the human body thanks to the advances on microelectronics with powerful information processing that can be used to monitor various health indicators (heartbeat, brain signals, pace, sleep, etc.). Although the future direction of developments is characterized by great uncertainty, this presentation will put forward possible scenarios.
David Carvalho, Founder & CEO of NAORIS, London, United Kingdom

Abstract
Cyberspace is a constantly changing space, highly disputed and a one of a kind environment without precedent in human civilization. If anything, it encompasses the traditional war-fighting domains, as an essential part of this is the need for complete inter-connectivity and insight into practically all aspects. With special focus on critical and highly regulated environments such as the energy industry and supporting infrastructure as value targets for an attacker.

The absolute penetrability of networks and technology in contemporary society means that everyone and everything are to some level connected even in the most remote of locations. It is at this moment that we as a society and as users stop to fully comprehend the authentic inter-connectivity of today's world due to its sheer complexity and start to overlook its vast vulnerabilities and risks.

Cyber-war is entering heavily into cyberspace creating increased worries to critical infrastructure and industry, especially in areas that are critical but new (thus widely untested by time), critical but legacy or are in budgetary crisis or geopolitical crisis.

In my talk I will cover the overwhelming risks and the mitigation strategies of future and current malicious real-world attacks that are currently undetectable and persistent, and list innovations that must swiftly be considered transversally in the most critical areas of society, its core-infrastructure and armed forces.

Some facts to have in mind as food for thought:
- Fully undetectable and persistent state-sponsored threats are one of the most omnipresent malicious threat agents in cyberspace and in high value targets that may lay dormant and can be activated in case of conflict or political tension across national critical infrastructures or similar environments.
- Amount of attacks and expertise of malicious actors in cyberspace continues to increase quadratically faster than defense techniques.
- Malicious infrastructures keep evolving their capabilities involving multipurpose configurable functions for traditional cyber-defences subversion such as anonymization, detection and encryption evasion.
- They're a top concern of governmental and commercial defenders, traditional cyberdefence environments do not seem to be able to protect such high value targets from advanced attacks.
- An incredible variety of kinds of hardware systems, architectures and networks are connected to form a worldwide cyberspace.
Bernd Datler, Director ASFINAG Maut Service GmbH, Vienna, Austria

Abstract
Traffic infrastructure as many other businesses has embraced modern IT and IoT long since. With billions of km driven on the network every year, hundreds of millions of journeys of both heavy goods vehicles and passenger cars modern traffic management wouldn’t be possible without solid IT-infrastructure and applications. The same holds true for modern road maintenance where winter service relies on sensor- and IT-based weather information and tasks are assigned to the workforce via IT-based work planning and billing solutions. In that respect infrastructure operators use pretty similar technologies like other industries but due to the size of the network sometimes at a larger scale.
With such an infrastructure in place of course business continuity and IT-security considerations play a significant role to ensure reliable business support through technology. This even more as the EU-directive on Network- and Information Security (NIS directive) comes into play. The directive obliges operators of essential services to ensure state of the art cybersecurity measures in place as well as processes to interact with national agencies in case of cyber security incidents.
Road infrastructure is of course among those essential services which brings many new challenges also for ASFINAG to tackle in the next years. An Information security management system is the basis for all the related activities that are aligned in a change program that has been started a few years ago. Cyber risk management complements the activities and guides the priorities. Blackout scenarios are also taken into account with focus on business critical topics such as communications but also fuelling and signalling.
What changes in the future with connected cooperative and automated mobility? Increasingly infrastructure and vehicles will act as an integrated environment more and more interacting with each other. Weaknesses on one part clearly affect the other parts of this ecosystem. Vehicle manufacturers, service providers but also infrastructure operators will need to constantly improve their security standards.
With cooperative systems sharing information between cars or infrastructure and cars this will become a hot topic over the next decade. Imagine a hacked car spoofing an emergency break warning to surrounding cars without necessity and without carrying out the maneuver. This could lead to a dangerous situation and is only one example of possible situations. Ensuring the verification of the origin and integrity of shared information will become vital in this very possible near future even more so as this information becomes crucial input for assisted and automated driving functions.
This also shows why cyber security is key to infrastructure operators. Not only the essential services have to be kept available for the public under a wide variety of circumstances. Cybersecurity incidents could directly have adverse effects on safety and therefore on the lives and health of the users of the service.
All these considerations set the scene for further IT-related developments and improvements of the technical systems supporting the business of infrastructure operators and need to be taken into account.