Hessian State Chancellery

Hessian Minister for Digital
Strategy and Innovation

HESSEN

Conference-Reader

Secure Smart Region Congress 2021

digitales.hessen

Contents

"Hesse on the way to become a Secure Smart Region!"

Dear Readers,

In July 2021, the district of Anhalt-Bitterfeld declared a disaster due to a cyber attack – the first of its kind in Germany. The incident has brought a new challenge into the public eye: digital attacks on our communities.

One thing is clear: we want smart municipalities, digital town halls and intelligent mobility. This is what will make Hesse more liveable, and more ecologically and climate friendly. To support this process, we have set up the Smart Region Hessen Office and established the Smart Region Congress. Here we advise and support municipalities in introducing digital technology. But the more municipalities digitize, the more cybercriminals look for openings. The question is: How can municipalities digitize quickly while maintaining a high level of cybersecurity?

We discussed this at the first Secure Smart Region Congress. We brought Hesse's municipalities together with experts from business and science. Central questions were: What should smart municipalities protect themselves against? How should they do it? And who can help them? We have heard many smart answers – including some from Israel, one of the world's leading nations in cybersecurity. The congress has taken us a big step further on the way to a Secure Smart Region Hessen. We have summarized the most important results and findings in this documentation. We will implement and further develop promising measures. Peter Beuth, the Hessian Minister of the Interior, and I are working together to achieve our goal of a Secure Smart Region Hesse.

Prof. Dr. Kristina Sinemus,
Hessian Minister for Digital Strategy and Innovation

"This congress shows how important security is for everyone involved in smart regions."

Dear Readers,

The first Secure Smart Region Congress of the Hessian State Chancellery, Department of the Minister for Digital Strategy and Innovation, with the support of the Hessian Ministry of the Interior and Sports, was very well received. This shows how important the topic of security is for everyone involved in smart regions.

We appreciate the valuable contributions from our administration's staff, from scientists and start-ups. Our guests from Israel have given us interesting suggestions on how secure smart regions and cities can succeed. All of this helps us to further advance digitization in Hesse.

I hope that you will enjoy this documentation presenting all the important ideas and impulses from the congress.

Peter Beuth,
Hessian Minister of the Interior and Sports

More information about all HMdIS offers:
https://innen.hessen.de/Sicherheit/Cyber-und-IT-Sicherheit

Keynotes

What visions exist in Hesse for the expansion of smart regions and cities? How can municipalities digitise themselves quickly and effectively while maintaining a high level of cybersecurity? And what challenges do municipalities have to protect themselves against when creating smart regions?

The keynotes provide some answers to these questions!

Secure Smart Hesse

Cyber and IT Security in Hesse – An Overview

Leaving the Silos Behind – Security Requirements for Smart Regions

Post-Quantum Cryptography for Privacy and Security of the Internet

Challenges for Secure Critical Infrastructures (CRITIS)

Keynotes

Secure Smart Hesse

"Hesse is to become a smart region by 2030 – a federal state with smart regions and municipalities as places of the future that offer a high quality of life and sustainability."

With the updated strategy "Digital Hesse – Where the future is at home", the goal is clearly defined. Hesse is to become a smart region by 2030 – a federal state with smart regions and municipalities as places of the future that offer a high quality of life and sustainability because they rely on digital applications in a smart, apposite, and innovative way and use data as the basis for their actions.

Hesse is already a hotspot for the European Smart Region development. Pilot municipalities such as Darmstadt, Eichenzell, or Kassel attract nationwide attention with their innovations. Whether urban data platforms, environmentally sensitive traffic control or digital tools for citizen participation: Smart region applications made in Hesse generate actual added value for the local citizens.

First steps have been taken towards this digital future: With the virtual Office Smart Region, a unit has been created that is available to the growing Smart Region community in Hesse as a platform and that provides attractive offers for exchange, networking, consulting, and knowledge transfer. These include, in particular, the annual congress „Digital Cities, Digital Regions", an information portal with a best practice database as well as various specialist information and FAQs. Through the promotion of smart municipalities and regions in the "Starke Heimat" program, Hessian municipalities have 16 million euros per year at their disposal for the development and implementation of innovative projects.

This way, it is possible to implement good ideas for the Smart Region of Hesse even faster and to spread the innovative power across the board of all Hessian municipalities.

Keynotes

Secure Smart Hesse

But with all the advantages that smart cities and regions have: The more digitized they are, the more attack surfaces cybercriminals have. Appropriate precautions can be derived from cybersecurity research. With the National Research Center for Applied Cybersecurity ATHENE based in Darmstadt, Hesse has an internationally renowned and brilliant example of cybersecurity research. A strong ecosystem in the areas of cybersecurity and privacy protection has formed around ATHENE in Darmstadt, for example, with numerous spin-offs and initiatives such as the Competence Center for Applied Security Technology. In addition, the German government named Darmstadt Germany's Digital Hub for cybersecurity in 2017.

Municipalities and companies benefit from the research results thanks to an efficient and practice-oriented transfer of knowledge. The House of Digital Transformation plays a special role here. As part of the Hessian Innovation Strategy, it links business, science and politics. This also as partner of the Smart Region Office.

To be both smart and secure at the same time, our municipalities can also count on start-ups and small and medium-sized enterprises that specialize in cybersecurity. The Public Procurement and Tariff Loyalty Act, recently amended by the State of Hesse, makes it easier to find common ground between the two, as it is now possible to take the aspect of innovation into account when awarding contracts. Specific information on smart procurement can be found on the homepage of the Smart Region Office.

Information

More information about all the offers of the Smart Region Office:
https://www.smarte-region-hessen.de/

Denis Liebetanz
Hessian State Chancellery
Hessian Minister for
Digital Strategy and Innovation
Devision Institutions of Digitization
and Smart Region

www.digitales.hessen.de

Sebastian Köster
Hessian State Chancellery
Hessian Minister for
Digital Strategy and Innovation
Devision Institutions of Digitization
and Smart Region

www.digitales.hessen.de

Keynotes

Cyber and IT Security in Hesse – An Overview

2021 has clearly demonstrated the far-reaching consequences of security attacks on (public) infrastructures, including declaring the first cyber disaster ever in Germany.

In Hesse, the topic of cybersecurity has been high on the agenda for many years: Our goal is a demand-oriented security architecture in which all actors from business, administration, science and across the federal, state, and local levels work together. Hesse currently holds a leading position among all 16 German states. We provide numerous targeted offers in the areas of prevention, detection, and reaction, but also networking, all of which we are continuously expanding. Our main initiatives are:

Offers for small and medium-sized enterprises (SMEs) and municipalities

The Hessen CyberCompetenceCenter (Hessen3C) as the central competence centre in the field of cybersecurity, including

- MIRT – the Mobile Incident Response Team primarily supports municipalities and SMEs in IT forensics on site
- Warning and information services on cyber and IT security aspects
- 24/7 availability and assistance to affected communities and businesses
- On-site consultations
- Implementation of information and awareness events

Special offers for municipalities

- Municipal Service Centre for Cybersecurity (KDLZ-CS): Tailored support and implementation of measures together with ekom21
- Hessian cyber defence training centre HECAAZ (under construction), including a mobile IT learning laboratory
- Consulting services in the field of information security management systems (ISMS), IT crisis management (IT KM) or business continuity management (BCM)
- Cybersecurity Summit: Security Congress for Municipalities in October 2022

Keynotes

Cyber and IT Security in Hesse – An Overview

Other projects

- Hessian IT Security Act (HITSiG)
- Hessian cybersecurity strategy
- Expansion of the state's internal cyber reserve
- Training and awareness campaigns in cyber and IT security, including funded professorships
- Practical exercises of IT crisis situations
- Establish an IT security mentality culture

Information
More information about all HMdIS offers:
https://innen.hessen.de/Sicherheit/Cyber-und-IT-Sicherheit

Ralf Stettner
Hessian Ministry of the Interior and Sports
Devision VII Cyber and IT Security
Administrative Digitization

www.innen.hessen.de

Keynotes

Leaving the Silos Behind – Security Requirements for Smart Regions

"We can live, communicate and interact securely in a smart region, provided that certain factors and their security relevance are being addressed."

From smart parking sensors and intelligent bus stops to smart street lighting and air sensors – all this must work hand in hand in a networked city / region. However, such an interoperability requires addressing three factors and their security relevance: visibility, the human factor and external threat scenarios.

Secure smart regions require visibility: you can't protect what you can't see. Having a clear idea of one's own IT infrastructure and individual smart devices must be ensured at all times.

It is also important to always keep an eye on the human factor. On the one hand, citizens must be involved in the process of creating smart regions, because only in this way can security be lived and internalized. On the other hand, the human resource must be leveraged as well, so that security can be exemplified from the outset, with know-how and knowledge.

Based on this, external threats must always be taken into account. This is done by implementing suitable methods, products, and measures.

These three factors should go hand in hand. Because even the best IT security system cannot offer any protection if it is not clear what is needed nor if there aren't any stringent actions undertaken.

However, when these factors are taken into account, security allows us to live, communicate and interact securely in a smart region. It can then help to identify, collect and classify the resulting "information nodes".

Melanie Eschbach
Check Point Software Technologies

www.checkpoint.com

Keynotes

Post-Quantum Cryptography for Privacy and Security of the Internet

Vulnerabilities of the public key infrastructure currently used to secure the Internet are enhanced with the development of quantum computers; with severe implications for privacy, security, and cryptocurrency. The distribution of information is a key solution for future security infrastructures. Quantum computers' development road map predicts a serious threat to today's encrypted data within less than a decade. This is an opportunity to reconsider the security of the Internet, based on the public key infrastructure architecture.

Having all information on a particular site or sent over a particular channel is a big risk for privacy. Forming targets for a man (or service provider) in the middle attacks, and penetrations attacks, which in turn, may lead to data leakage and ransomware attacks that are experienced every day. Information distribution can serve us today inefficient solutions for data in motion and data in rest. Ownership of information is preserved when sending a credit card number, sending a random number through email, and a random number through SMS, such that their XOR gate is the actual number. Storing photos in your own computer / server may risk data leakage and / or ransomware attacks, storing in Google Drive and alike, yield a trust in a single entity (and all the employers of the entity) and loss of data ownership, hence, a multi-cloud solution, each cloud storing random numbers is preferred. Blockchain distributed trust complements the above solutions allowing private logic contracts.

Summary

Quantum computing offers the chance to rethink the security of the internet - let's seize it!

Prof. Dr. Shlomi Dolev
Ben-Gurion University of the Negev
Be'er Sheva, Israel

www.cs.bgu.ac.il

Keynote

Challenges for Secure Critical Infrastructures (CRITIS)

Smart regions and cities are extremely dependent on the security of their critical infrastructures (KRITIS) – be it in the digitization and networking of communication, mobility and transport, health or energy. Since critical infrastructures tend to function almost always, and because it would hit an unprepared population, the consequences of a potential failure would be all the more drastic. This supposed contradiction (secure infrastructures will lead to great damage in the event of potential failure) is referred to as the "vulnerability paradox": "To the extent that a country is less susceptible to disruption in its supply services, every disruption has an even greater impact" (Federal Ministry of the Interior).

For smart regions and cities, it is therefore important to avoid attacks and disruptions in the best possible way, but at the same time they need to prepare well for dealing with them. Risk and crisis management can provide for the following steps:

- Define hazard categories
- Determine the level of protection
- Derive varying scenarios
- Weak point analysis
- Define protection objectives and associated measures
- Determine the required need for action
- Implementation and review

The PEASEC Chair of TU Darmstadt and the SecUrban Research Department of ATHENE conduct research on these topics. For more information, see www.peasec.de and and www.securban.athene-center.de.

Prof. Dr. Christian Reuter
ATHENE / TU Darmstadt

www.securban.athene-center.de

Workshops

Based on advance feedback from the participants, the interactive workshops took up three very exciting topics and contents:

Data Platforms and other Digitization Projects

Support by Civilian Relief Forces in Large-Scale Cyber Disasters

Governance of Cybersecurity for Municipalities

Participants had the opportunity to delve deeper into the topics and contribute their challenges and requirements.

Workshops

Data Platforms and other Digitization Projects

Something is happening in our country. That is the result of Bitkom's ³rd Smart City Index. The index examines the degree of digitization of German cities with a population of 100,000 or more in various categories ranging from intermodal mobility and citizen participation to energy and the environment and digital administration. There are many dynamics in place, especially with regard to the various digitization trends. While some cities are extending their lead, others are still in the starting blocks for their smart city strategy. This year's frontrunners include Hamburg, Cologne, Karlsruhe, Munich and Darmstadt.

In recent months, the top performers have devoted themselves to the introduction of smart city data platforms, which form the technical heart of any digital city. Darmstadt went live with its data platform in February 2019. It bundles and visualizes various sensor data of the city in real time and thus ensures transparency about the city's events. Data analyses and the establishment of causalities between the data lead to gaining new knowledge and enabling improvements. An example of this is the connection of traffic data with environmental data and events in the urban area. Here, the data platform provides the basis for contributing to the improvement of traffic flow and air quality via traffic forecasts and intelligent traffic control. A real win for everyone!

Summary

Data platforms are the heart of a smart city. Through the availability and evaluation of networked data, it is possible to support and accelerate necessary urban decision-making and planning processes - a real benefit for everyone!

Simone Schlosser
Digitalstadt Darmstadt

www.digitalstadt-darmstadt.de

Michael Pfefferle
Bitkom e.V.

www.bitkom.org

Workshops

Support by Civilian Relief Forces in Large-Scale Cyber Disasters

Rapid action is required when a major cyber emergency situation occurs. With the Cyber Emergency Response Teams (CERTs) and Mobile Incidence Response Teams (MIRTs), government emergency units for cyber incidents are already in place. But what if the existing capacities are no longer sufficient?

Additional support could be provided by trained volunteers. For smaller cases, the Cybersecurity Network has been established in Germany, with digital first responders offering telephone assistance to SMEs. However, such a solution does not yet exist for large damage situations. A volunteer organization could provide rapid help for recovery, analogous to the existing aid organizations. The expert network AG KRITIS has already developed corresponding suggestions, and the coalition agreement of the new government provides for an expansion of cyber capacities within the Federal Agency for Technical Relief.

The Cyber Unit of the Estonian Defence League shows that the involvement of volunteers can succeed. The volunteer organization was founded by supporting companies and experts in response to the large-scale cyber attacks in 2007.

Information

In order to prepare critical infrastructures for crises in Germany as well, the PEASEC chair at TU Darmstadt conducts research on the requirements of municipalities and infrastructure companies with regard to major cyber damage situations. People in this field of activity are cordially invited to provide support as interview or discussion partners. Interested parties can register under this link.

Jasmin Haunschild
ATHENE / TU Darmstadt

www.securban.athene-center.de

Workshops

Governance of Cybersecurity for Municipalities

Kirstin Scheel and Michael Kreutzer, both ATHENE, presented the results of a project that was supported by the Hessian Ministry of the Interior and Sports. They identified five preventive measures that can help mitigate the risk of cyber incidents during the process of developing towards smarter communities. These are based on the principles shown in the graphic below:

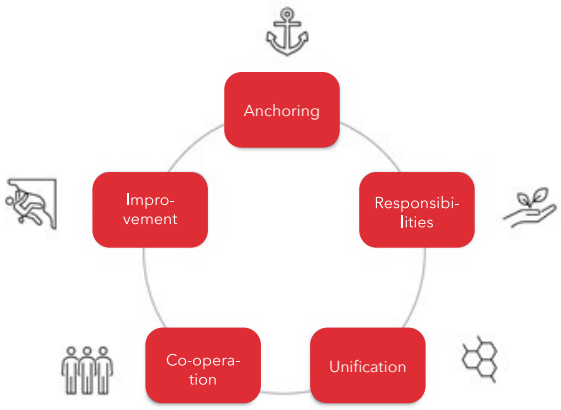
anchoring,

responsibilities,

unification,

co-operation and

improvement.



Cybersecurity must be anchored at the highest level in an organization. Top management must be aware of the need for security as the cornerstone of all digitization projects.

Responsibilities must be clearly assigned. In addition, these responsibilities require adequate resources to bring them to life.

Another central idea is the unification of systems and processes across organizational units. For example, many cases of malware infestation can spread via systems that have not been segmented properly.

Operational co-operation and cross-divisional collaboration are also important to use resources efficiently and effectively.

Dynamically changing environments require continuous improvement. Learning from internal and external mistakes is essential to keep up with these developments.

Dr. Michael Kreutzer
ATHENE / Fraunhofer SIT

www.athene-center.de

Best Practices

How can secure smart regions succeed? What preconditions must be created in advance? How important is security by design for secure smart regions? What exciting research projects and start-ups are there in this sector? What influence does participation have on the development of smart cities and regions? And what can we learn from Israel here?

These and other questions were addressed and answered in the Best Practice Sessions. On the following pages you will find the short and interesting summaries.

Best Practices

Living Labs and Ecosystems

The smarter you are, the more vulnerable you get. As smart regions aim to create a safer and more secure environment, they need to protect their infrastructure and data. This involves finding and deploying innovative new solutions. To do so, two things have proven to be best practice:

Firstly, it is beneficial for communities to test new and innovative solutions in living labs such as the one created in Tel Aviv. The idea is to pilot applications in a protected but real life environment.

Secondly, it makes sense to either initiate or tap into innovation / start-up communities. In some instances, it can even make sense to put out dedicated calls for solutions. In Tel Aviv this is supported by impactful start-up programs such as the one run by Tel Aviv based accelerator CityZone.

CityZone's program taps into one of the world's most prolific and innovative start-up ecosystems – It connects start-ups, cities and industry leaders to tackle joint challenges. It provides access to sandboxing, to finance and exchange, e.g. in its "city-corporate start-up"- roundtable.

Recommendation:

- Use living labs and accelerators to pilot applications in a protected but real life environment.
- Either initiate innovation / start-up communities or use existing ones.

Gaby Kaminsky
CityZone

www.city-zone.co

Best Practices

Improving Citizens' Safety and Smart Cities and Regions' Resiliency

"How do you not only protect the safety of your citizens, but also ensure the sustainability and resilience of your smart city / smart region?"

Smart Regions and Smart Cities infrastructures and people are vulnerable being exposed to a variety of threats. On the one hand, there is the continuous danger of cyber attacks hitting on the infrastructure. On the other hand, there are environmental / ecological factors such as air and water pollution, heatwaves, storms, floods or even wildfires. Consequently, a key question for smart regions is how to enhance citizens' safety and the city's / region's sustainability and resiliency?

On an organizational level, each municipality should establish an emergency situation manager and a C&C centre. This function needs visualization and alerts and permanent access to all relevant information. Their job includes detection and prediction as well as response. Emergency management should be handled automatically with possibilities of manual interventions. Solutions such as IPgallery leverage the connected infrastructure and enhance it with AI based services. We provide insights on a day-to-day basis for smaller incidents and the full scope of technology to handle larger emergency situations.

Avihai Degani
IPgallery

www.ipgallery.com

Best Practices

Smart AND Secure Digital Cities

The Digitization Unit of the City of Offenbach has two tasks: to promote the smart city transformation of Offenbach, and the administration's digital transformation together with the IT departments of both the city and the municipal utilities departments. Key IT-security challenges are:

Open-source-software as a component of the digitally sovereign smart city: The security-oriented (further) development of the software must be ensured centrally (Centre for Digital Sovereignty of Public Administration).

Encryption: Simplification and centralization can relieve municipalities, for example by implementing a state CA (Certification Authority).

Growing "business models" such as ransomware-as-a-service and insufficient digital security awareness: more central, low-threshold learning opportunities and appropriate financial resources are needed.

Recommendation:

Best practice examples of data protection in the smart city include collaboration tools such as the Bundeswehr's OS Messenger and the Open Diffix project, which promises an easy anonymization of data sets.

Anne Schwarz
Stadt Offenbach

www.offenbach.de

Best Practices

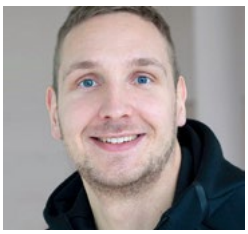
Cybersecurity in Smart Regions – A Matter of Transparent Figures

Many IT infrastructures have grown in a more or less structured way over the years. The result: Despite an increasing awareness about IT security, companies, organizations and municipalities often do not have a complete overview of the entirety of their IT systems, for example websites, network and software. This is why those responsible often do not know how secure their systems are and how well they are protected against attacks.

Solutions that automatically scan and document all IT assets of an organization can be used to get an overview of an organization's own IT infrastructure and IT-security status. This, in turn, will allow the organization to prioritize required security activities.

In Hesse, the start-up LocateRisk offers such a solution: it is used to record and evaluate IT infrastructures from an external perspective and summarize them in a report with prioritized recommendations for action. Municipalities can arrange for a non-binding initial analysis and, based on this, follow-up with a free consultation under www.locaterisk.com

Summary:
Get an overview of the entirety of your IT systems. Only then can you initiate targeted measures to protect them.



Lukas Baumann
LocateRisk

www.locaterisk.com

Best Practices

Participation as Key Element of Smart Region

The digitization of smart cities, communities and regions has the potential to change the way decisions are made. In concrete terms: For us, smart regions mean that politics and administration use the knowledge of citizens and other stakeholders. The constructive involvement of a region's citizens creates better decisions, more acceptance and a sense of community. This is what makes a smart region. We accompany regions on their way to the smart region with our „Insights Process"-method and CrowdInsights platform. More information at this link.

Recommendation:

Citizens, as users and residents of a city, represent the central element of a smart city. Involve them and use participation as a central element of smart city development!

Dominik Wörner
CrowdInsights

www.crowdinsights.de

Best Practices

Working Together towards a Sustainable Security Culture

"We want to help make digital Germany more secure step-by-step and we are starting in Darmstadt."

Most successful cyber attacks start with the human factor, for example phishing. If you want to protect yourself successfully against this, you do not only rely on technology, but especially on a good security culture. Ideally, organizations therefore educate and sensitize their employees through awareness trainings.

With the free "Stay alert" campaign, the city of Darmstadt and IT-Seal developed this idea further. It launched the first local cybersecurity campaign and offered security trainings for its citizens. The goal: a sustainable security culture with a broad reach. The idea: the more people are well trained, the better the protection of society.

Under the motto "You are the firewall", the campaign focuses on multiplication effects. The content is designed for everyone and raises awareness for dealing with their own IT, social engineering, email security / phishing, social media and passwords.

"Stay alert" was developed by IT-Seal, a leading awareness specialist in the Security Valley Darmstadt.

More information at www.darmstadt.bleib-wachsam.de

Alex Wyllie
IT-Seal

www.it-seal.de

Best Practices

Protecting the IoT - Solutions for Connected Systems

Supply chain software attacks are becoming a preferred vector of attack for organized crime. SolarWinds, Microsoft, and quite a few others were used by organized crime as conduits through which they attacked multiple customers of those companies, by exploiting software vulnerabilities that were discovered and, in some cases, even maliciously and actively introduced. Other vulnerabilities were not intentionally introduced. They originated from developer error, and from the convoluted supply chain which many software providers have and which complicates the process of identifying 3rd-party components and updating them when a vulnerability is discovered.

Smart cities need to tighten supply-chain-related cybersecurity measures. An important component in this effort is identifying commercial software components and their associated vulnerabilities. IoT suppliers need to scan software images for known vulnerabilities, configuration risks, unsecure binaries, bad passwords and more.

Summary:
Supply chain software attacks are becoming increasingly common. Municipalities must therefore pay special attention to protecting their IoT.

Gregor Knappik
Karamba Security

www.karambasecurity.com

Best Practices

Secured 5G Traffic Management Solution

"With secure and smart traffic control to more efficiency, environmental protection and quality of life without restricting citizens in their mobility."

25 kilometres per hour was the average travel speed by horse. In Berlin it is currently 17 kilometres. The reasons: more cars and an infrastructure that was not build for the current amount of traffic. The overcrowded system leads to congestion, lost productivity and excessive pollution. To tackle these issues, smart cities are well advised to implement effective intelligent traffic management systems. Smartly used, these systems will not only reduce traffic jams but also enable communities to provide specific means of traffic, e.g. for bicycles or public transport.

One example of such a system is the AI-based software from the Israeli start-up ITC. The software integrates with existing road cameras, allowing it to access a wide range of data to identify the clustering of traffic patterns. In this way, congestion patterns can be predicted and directly alleviated through a customized traffic plan - long before traffic jams occur. At the same time, intelligent traffic solutions prepare smart cities for future technological developments such as Connected Vehicle and the full deployment of 5G networks.

Dvir Kenig
ITC - Intelligent Traffic Control

www.itc-israel.co.il

Best Practices

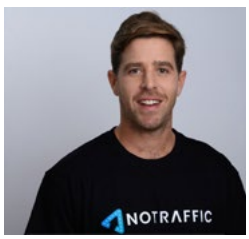
Increased Safety through Autonomous Traffic Management

Autonomous traffic management is one of the deployments in a smart region that will create an immediate impact. By significantly reducing congestion and applying overall smarter traffic management, communities first need to create digital grids that share data and information.

However, for many cities the challenge remains that their intersections are often manual and disconnected. To overcome this, companies such as NoTraffic have created platforms that are fast to deploy and leverage grid data collected by sensors, using connected edge computing and cloud-based management. The data can be complemented by those from additional data sources to enable fully automated traffic management, e.g. for the optimal decision to change the light or prioritize first responders to accidents. The impact results in less delays, significantly less emission and unlocks opportunities for new connected services. The benefits are increased safety and clear value for money.

Recommendation:

Leverage existing resources and leverage them to create a valuable contribution in the areas of safety, traffic management and navigation.



Matan Nir
NoTraffic

www.notraffic.tech

Best Practices

Application-Oriented Research Funding in Hesse

The Devision Cybersecurity Innovation Management at the Hessian Ministry of the Interior and Sports pursues two major goals: One of them is to combine technical needs and research in application-oriented (meaning directly usable), concrete and projected initiatives. The other one is about knowledge transfer, networking and the expansion of a narrow ecosystem. The offers are aimed specifically at the Hessian security authorities and the municipalities.

The four pillars of the Devision Cybersecurity Innovation Management:

1. Strategic governance, including the Cybersecurity Advisory Board
2. Research in the ecosystem with its own funding guideline, funding calls and a framework agreement for research
3. Event formats such as lecture series, podcast series, municipal cybersecurity days or workshops with market explorations
4. Federal and Europe-wide contacts and networking, for example with the transnational platform cybersecurity research under Hessian leadership, the EU Competence Centre in Bucharest or the Agency for Innovation in Cybersecurity, among others

More information at:
https://innen.hessen.de/Sicherheit/Cyber-und-IT-Sicherheit/Innovationsmanagement-Cybersicherheit

Dirk Dohn
Hessian Ministry of the Interior
and Sports
Devision Cybersecurity
Innovation Management

www.innen.hessen.de

Panel

The final panel focused on the practical implementation of safe smart measures for smart regions and cities and their preconditions. The panellists from Israel and Germany reported on their direct and indirect experiences.
The panel included:

Johannes Rothmund
Mayor of Eichenzell

www.smartcity-eichenzell.de
www.eichenzell.de

Dr. Steven Arzt
ATHENE / Fraunhofer SIT

www.athene-center.de

Jochanan Sommerfeld
7CI

www.sevenci.com

Rami Efrati
MSF Partners Innovation

www.msfpartners.com

Panel

Statements

» Johannes Rothmund

"Smart offers are extremely important for the attractiveness and efficiency of our community. At the same time, we want to protect the data of our citizens and offer the highest standard in the areas of data security, data protection and data sovereignty. For example, we use a multi-certified data centre on site.

We experience that data protectors often have a critical view of new, smart offers – also because there is a lack of experience with them. So, we are often slower than we want to be. This is why we are pursuing a more agile approach to pilot projects: when planning them, all aspects of data protection are of course taken into account, they then get implemented and, in cooperation with the Hessian Data Protection Officer, we check where we still need to improve. This way we ensure together and early on that we are on the right track."

» Jochanan Sommerfeld

"Security is not a function but a characteristic of every system, environment and entire solution. Hence, it should be viewed similarly to quality and be considered at all stages of a lifecycle, from ideation to deployment and maintenance. However, since there are a variety of sectors and verticals, as well as a multitude of technologies involved in the journey to be a smart region, it is essential to simplify the complexity as much as possible. A journey laden with complexity is inevitably doomed to fail. In particular, I mean following these principles:

- Standardization and best practices
- Practicing YAGNI (You Ain't Gonna Need It) results in leaner and more focused apps
- Design for scale
- Treat security as a characteristic and not a feature
- Identity management"

Panel

Statements

» Dr. Steven Arzt

"For new IT projects, a configurable framework should be used right from the start to enable systematic risk assessment. Established concepts already exist to estimate the expected attackers, their attack targets, motivations, conditions, etc. On this basis, countermeasures can be planned, evaluated, and decided. Key questions are: What needs to be secured and which measure is appropriate in terms of costs and benefits? Reusable processes and building blocks for security and data protection are essential for countermeasures. This avoids reinventing the wheel again and again.

Software is an issue in almost all public IT projects. SecDevOps processes are usually in the foreground, for example by using automatic code scanners as a measure to ensure at least a minimum level of software code quality."

» Rami Efrati

"As a country we have the reputation of being very strong in improvising, which is often very beneficial. But with cyber, we do not improvise: Cyber is part of our culture. That means, we are not just looking at this based on one problem. It is embedded into awareness, resilience, and other considerations. It is based on experience and best practice. We live cyber and privacy by design and once you get to this point, you are able to speed up a lot. So, my three best practices are:

1. Take cyber as your foremost priority: If you don't protect yourself from cyber attacks, you won't protect your privacy.
2. Take a strategic approach and prioritize what is the most important to start working with.
3. Learn to focus on effective solutions in a short time."

Imprint

Office Smart Region:

State Chancellery of Hessen
Minister for Digital Strategy and Innovation
info@smarte-region-hessen.de
www.smarte-region-hessen.de

Imprint

Publisher
State Chancellery of Hessen
Minister for Digital Strategy and Innovation
Georg-August-Zinn-Straße 1
65183 Wiesbaden

Editorial:
Ute Richter, Lena Kress
ATHENE project Digital Hub Cybersecurity

Design:
Fraunhofer Institute for Secure Information Technology SIT
www.sit.fraunhofer.de

Image References:
Cover: istockphoto / metamorworks
Pictures of the contributors have been made available to us.

Exclusion of election advertising:

This publication is issued as part of the public relations work of the Hesse State Government. It may not be used by parties, canvassers or election workers during an election campaign for the purpose of election canvassing. This applies to state, federal and local elections. In particular, the distribution at election events, at information stands of the parties as well as the insertion, printing or pasting of party political information and advertising material is abusive.It is also forbidden to pass them on to third parties for the purpose of election campaigning. Even without a time reference to an upcoming election, the publication may not be used in a way that could be understood as partisanship of the state government in favour of individual political groups. The above-mentioned restrictions apply irrespective of when, by what means and in what quantity this publication is sent to the recipient. However, parties are permitted to use the publication to inform their own members.