



eurofunk news

ISSUE
Nº 03

CONTROL CENTER TECHNOLOGY IN THE CLOUD

One of the many topics
you will find in this issue.

BSI IT BASELINE PROTECTION

eurofunk - your professional
partner for implementation.

ACTIVE MONITORING

Detecting faults before they
become problems.

IP EMERGENCY CALL

How is an emergency call
transmitted via IP?

Emergency call handling by artificial intelligence from a secure location in the cloud. – Fiction, contradiction or tangible future?!



AI or artificial intelligence is here and here to stay – we all agree on that. What is far from decided is the relevance AI will have in the field which is why, across industries and applications, it is undergoing intensive R&D.

There is a certain appeal to the idea of providing a machine with a knowledge base – an education so to speak - from which it can derive further information and ideally develop the ability to make decisions in only fractions of a second.

The key question in all fields of activity then becomes: when are the decisions good enough - accurate enough - to measure them against the experience of an expert? How human, or humane, can a machine be and how much empathy can it display towards a person in need of help?

This often raises further questions:

Will AI be able to replace operators in the future? Are machines able to accept emergency calls or independently manage incidents? Will the chatbots we see in use on various websites ever reach a stage where they can communicate effectively with people in distress? Are there specific instances where this might be considered, or, looking shorter term, are there AI functionalities available now that can assist us?

The attempt to answer these questions often raises more:

How do we locate AI? Can we place it within a control center or must the intelligence come from the cloud? Is the cloud private, public or a hybrid of the two?

The watchword cloud typically raises further concerns. We think about things like security measures for the cloud and the standards that are establishing themselves for security control centers. Is an ISO/IEC 27001 certification adequate for operators and system suppliers? What other standards are being set by the Federal Office for Information Security (BSI) for the Federal Republic of Germany? Is it possible to develop a framework that simplifies the certification process for operators of security control centers?

Answers to and perspectives on these and many other interesting questions can be found in this edition of the eurofunk NEWS. We would also be happy to discuss these exciting topics with you personally.

We hope to peak your curiosity with the following pages and wish you inspiration and pleasant reading!

Christian KAPPACHER – CEO



Contents

INNOVATION

- Active Monitoring 06
- AI in the control center environment 08
- Cloud Hosting - future of control center technology? 10

COMMUNICATION

- IP emergency call 12
- Digital Radio Connection in Germany 16
- Communication solution emc^{WEB} 18
- Automatic triggering of digital radio alerting 19

PRODUCTS

- Dispatch Center Interface 20
- Ergonomics 22
- Modernization at ILS Nuremberg 26
- eurofunk Automatic Call Distribution 28

COMPANY

- BSI IT baseline protection 29

Active Monitoring

DETECTING FAULTS BEFORE THEY BECOME PROBLEMS.



Christoph SEIDL



System availability is vital for control center operations. Traditionally, monitoring systems were managed by inhouse system administrators with support from the eurofunk service team for fault resolution. When the system administrator was absent, it was not uncommon for early warning faults to remain undetected if the impact on control center operations was minimal.

In response to this common problem, eurofunk took steps to establish active monitoring within the service division, placing a highly specialized Operations Team at eurofunk headquarters to provide real-time system monitoring and system state analysis.

The potential for adding value was a key element of the concept. To decide which aspects of the system should be actively monitored, several hundred faults were analyzed according to

specific criteria. Analysis showed that 64% of all faults could be detected in the early stages and the root cause ascertained much faster. Since most systems have built-in redundancy, faults do not necessarily have an immediate effect on system performance. These faults can be detected and fixed during active monitoring before they become problems. This is similar to technical monitoring measures where warnings are generated before an actual malfunction occurs (e.g. full hard disk partitions).

Detailed analysis:

- 43% of faults can be identified through active monitoring
- 21% of faults could be potentially identified through additional monitoring

Active monitoring fulfills two main objectives:

Improved Monitoring

Systematic improvements to all applications make it possible to retrieve and evaluate information in greater detail. Storage of historical data will lead to the identification of trends and outliers in the future. The resulting improvements will be continually fed back into eurofunk products and rolled out to customers on an ongoing basis.

The Operations Team

eurofunk service now includes a dedicated team for continuous monitoring and monitoring system optimization. Additional processes within the service department ensure we are able to react to critical failures around the clock. Active monitoring has completed a pilot phase of extensive testing at two customer sites.

Information security and data protection are paramount. The permanent link to the control center - essential for active monitoring - is subject to the highest security standards. The link is via a secure and encrypted connection with priority being placed on state-of-the-art encryption methods. System security is handled by eurofunk's ISO/IEC 27001 certified service organization.

eurofunk active monitoring in a nutshell:

- GDPR compliant
- Checks the processing of personal data
- Assures security of information through an ISO/IEC 27001 certified service organization

Through detailed preparation and an open and transparent approach eurofunk active monitoring received the go-ahead from a nationwide police organisation: clear evidence of the reliability and integrity of our designed solution.

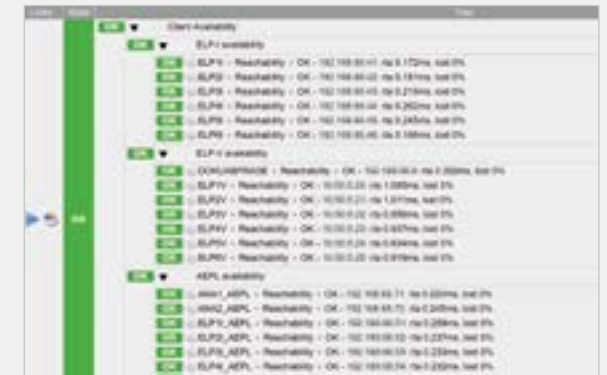


Fig. 1: Aggregations are used to combine individual monitoring events into an overall view of system state.

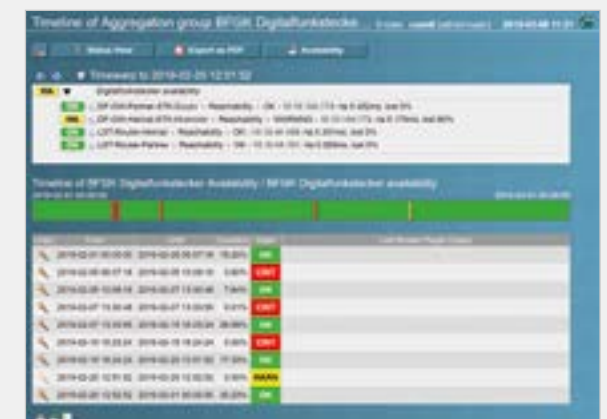


Fig. 2: The timeline displays the availability of individual components. It is also possible to analyze the cause of a fault at a later date.



Fig. 3: The system provides a simple overview of complex technical relationships.

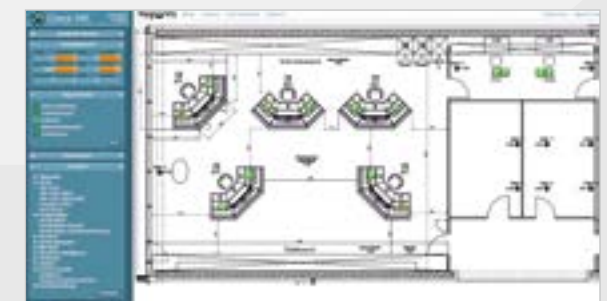


Abb. 4: Overview of the control center.

AI in the control center environment - hype or added value?



Christian REPASKI

If reporting on the subject is any indication, the number of projects benefitting from artificial intelligence (AI) is on the rise. We are pleased to observe this phenomenon in research projects that eurofunk is involved in as well; AI is opening up new possibilities and alternative approaches to standard solutions.

From the first moments of our existence, humans absorb vast amounts of information, every second, through our sensory organs. We process this information, either consciously or unconsciously, using the knowledge we gain in our future actions and decision-making.

Similarly, the systems used in control centers (communication and incident management systems) record large amounts of information from every call or incident which is handled. Until now, this has been earmarked mainly for statistical purposes.

Artificial intelligence is now so advanced that it can independently generate images or videos of non-existent persons or objects, autonomously write entire newspaper articles or communicate with people in a deceptively realistic way (chatbots). The area in which most advances have been made is image and speech analysis. AI has already found its way into our homes and into our working environment, making everyday life that bit easier and safer.

Despite the increasing number of data interfaces and sensors connected to the „information broker“ control center, verbal communication is still used to accept and process most inci-

dents. The natural follow-on is to consider how emergency call and incident processing can be optimized with the help of speech analysis and transcription (e.g. speech-to-text) to the benefit of both caller and call taker.

eurofunk is currently working on a solution that uses both on-site and cloud-based speech analysis to simplify and streamline emergency call acceptance and processing. While the operator concentrates fully on the call, AI can deal with the simultaneous conversion of the spoken content to text. The addition of foreign languages and local language translation is also planned. Using keywords (e.g. address) AI will automatically recognize and insert information into the appropriate data field. The software will analyze the content of an on-going conversation and suggest suitable indicators or keywords. Life-threatening illnesses will be identified and flagged up to the operator. AI will also give the operator suggestions for the collation of further important information to assist with the progress of a call.

In spite of all the technological progress and support provided by AI, the role of people in the control center environment will remain. Human creativity and the ability to adapt spontaneously to new situations are skills which a computer or machine will not be able to master readily. Even with a standardized and well-structured emergency call acceptance procedure, emergency call processing cannot be carried out without people. There will always be exceptional situations requiring human creativity and intuition.

Follow the links to try out **speech-to-text** for yourself:

- Google Speech-to-Text
<https://cloud.google.com/speech-to-text/>
- Microsoft voice recognition
<https://azure.microsoft.com/en-us/services/cognitive-services/speech-to-text/>



AI: What is it all about?

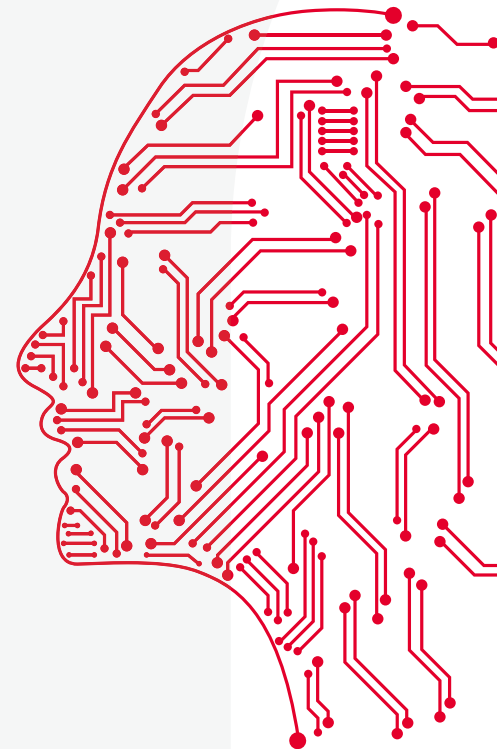
A.: The human brain is still not fully understood. We know that it can store large amounts of information and carry out calculated decision-making processes with the aid of training and guidance. Similarly, machines and computers equipped with AI are „fed“ with large amounts of information (machine learning) and, over time, they develop the ability to make recommendations and self-validated, autonomous decisions. This is what the AI learning process is all about.

Would you like to help us enrich the AI experience in control centers?

Are you prepared to make emergency call data available to us for „learning“ purposes?

If so, then please get in touch with me!

✉ crepaski@eurofunk.com



Cloud Hosting – could this be the future of control center technology?

The control center market and above all BOS is undergoing rigorous restructuring. Individual control centers for fire departments, the emergency services and the police are being consolidated into what are known as integrated control centers. These integrated control centers are, in turn, experiencing an unprecedented period of cross-board cooperation and the creation of control center networks.

With a view to efficiency and cost reduction, eurofunk is focusing on finding a cloud solution for control centers.

Control center technology in the cloud

Cloud solutions are familiar to many of us from their use in the private sector (e.g. Dropbox, iCloud). What you may not know is that cloud solutions also offer future potential for control centers. A classic cloud is a data center that provides software and services centrally via a network. This can be used simultaneously from several locations. The underlying hardware, or more precisely the allocated resources, can be adapted dynamically which means that both computing and data capacity can be adjusted as needed.

Private Cloud Solutions

There are several ways to provide cloud resources. For control center technology we would employ the so-called private cloud. In contrast to public cloud solutions, the private cloud is only available in a private, internal network. This means that without a closed Virtual Private Network, or VPN, it cannot be accessed by the general public via the Internet. VPNs offer a high degree of control and security which makes the private cloud a suitable solution for organizations with strict data security and data processing requirements.

While standard control center networks provide one server landscape per control center, cloud solutions for control center servers are operated centrally with redundant executions, either in one or in several data centers.

For the individual control center, the costs for server operation, data center maintenance, general data processing and other associated costs can be eliminated. Hardware and software updates need only be carried out at one central location. Changes to external interfaces must only be made once and modifications to the environment can be addressed in a timely manner.

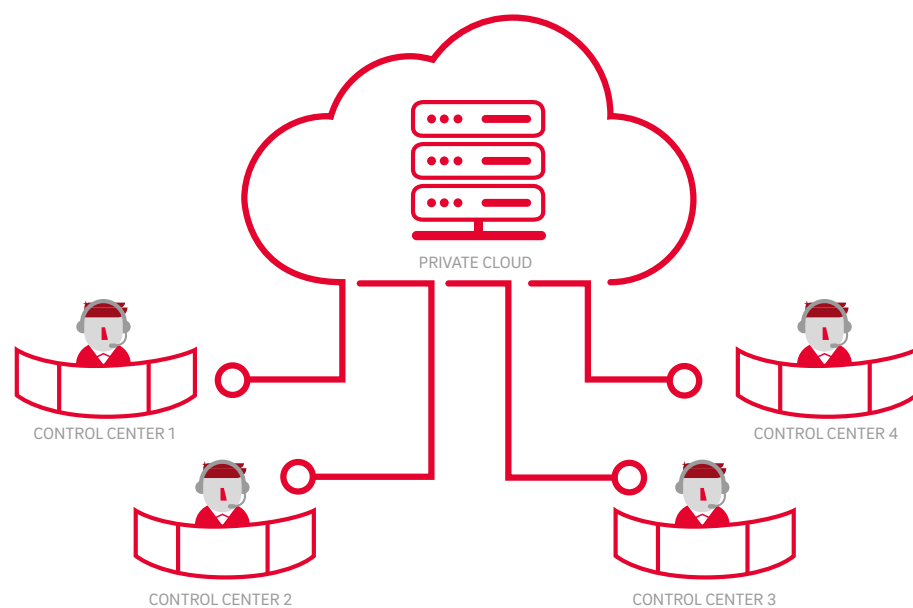


Fig. 1: Private cloud solutions for control center alliances



Christoph SEIDL

Hybrid Cloud Solutions

The collection and distribution of information play a vital role in control center activity. The technologies used are all IP technologies. Telephony (VoIP) as well as alarm systems and alarm services are moving away from serial or PCM-based protocols towards IP protocols. As a result, the idea of complete network isolation must be reconsidered and replaced with an integrated solution of secure, state-of-the-art technologies. At the same time, the local connection loses relevance because the functionality is tied to physical connections. This gives the opportunity for hybrid scenarios that provide quick resolution for application issues.

With a hybrid cloud solution, essential system components are hosted in a private cloud. The flexibility and added functionality of a public cloud is used for certain scenarios:

■ Training and Test Systems

These are systems that are only needed at certain times. In conventional situations, control centers would purchase hardware and software for training and testing purposes. With a hybrid cloud solution, control centers would save the purchasing costs and be able to access their systems as needed.

■ Support for Situation Centers

Local situation centers are used for complex incident scenarios such as natural disasters or demonstrations. In the case of area scenarios, the situation centers of different organizations can be distributed over several locations. For these scenarios, assistance can be garnered by means of hosting in a public cloud. The hybrid approach ensures close cooperation and an active exchange of information among control centers.

These are just two examples of cost reduction on the one hand and expansion of control center functionality on the other. eurofunk can, as usual, provide for the implementation and maintenance of the systems and make sure they remain functional and well-monitored.

Control center suite eOCS is the solution for the cloud

The eurofunk Operation Center Suite (eOCS) was designed from square one to operate in a cloud environment (both private and public). The consistent use of so-called **cloud native technologies** makes it possible to provide new instances quickly and easily. In addition, these technologies enable dynamic scaling according to current requirements. In crisis situations, for example, situation centers can be set up quickly to support the control center.

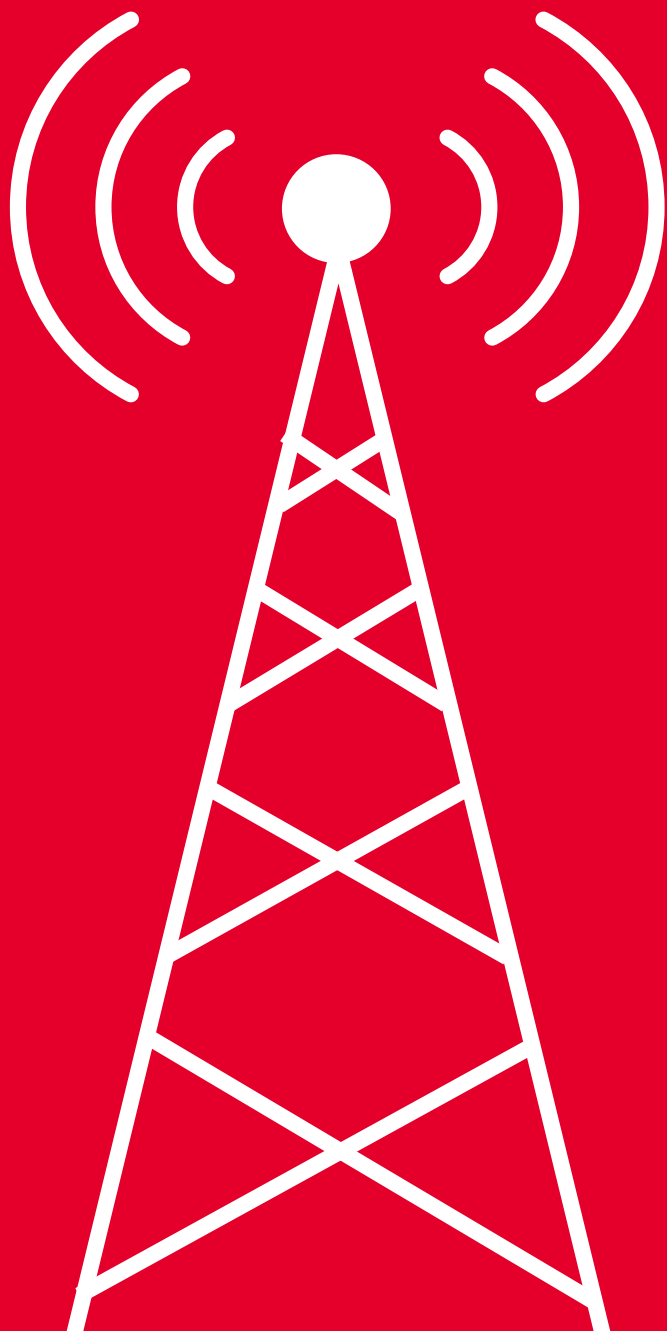
Advantages of cloud solutions for control centers

As mentioned previously, the control center environment is changing significantly in terms of organizational structure and thus also in terms of efficiency and cost optimization. The ability to operate control centers from a cloud could, in future, make the quick realization of a nationwide network significantly more straightforward. The cost reduction due to the elimination of separate data centers per control center is considerable. Thanks to central software and hardware locations, control centers acting as part of a network are always on parity. The network solution also offers advantages in terms of representation, support and organizational agility.



Find out more about eOCS on our website:
www.eurofunk.com/products/command-control/eocs/

IP emergency call for the eurofunk communication solution IDDS UCiP



The eurofunk Communication Solution IDDS UCiP is a modern, intuitive IP communication system designed for the control centers of tomorrow. ISDN technology, until now the telephony standard, is being replaced by Voice over Internet Protocol (VoIP) or "all IP".

For IDDS UCiP this means integrating new features such as IP emergency calls into the communications solution according to German **Technical Guidelines for Emergency Calls 2.0**, Federal Network Agency 2018.



Günter DUTZLER

The handling of IP emergency calls in IDDS UCiP requires the following:

Session Border Controller (SBC)

The SBC acts as a separator between the external VoIP connection and the IDDS UCiP system. All Session Initiation Protocol (SIP) trunks from telecom providers and control center IP telephone systems (PABX) operate through the SBC for security and interoperability reasons.

The SBC acts like a router between the IP telephone network and the IDDS UCiP system. It prevents unauthorized calls from accessing the system and can be considered a cornerstone of IT security. As the SBC supports a large number of services (e.g. encryption, speech transcoding, signaling protocol translation), it is possible to link different telephone systems simultaneously. eurofunk supplies the SBC core component for the IP connection and customizes the external configuration according to the networks to be connected. The SBC distributes the SIP connections to the relevant IDDS UCiP Emergency and Telephone Gateways (ETGA). One SBC cluster is supplied for each control center/technical node with IP telephony connection.

It should be noted that the SBC is only used for VoIP-based telephone systems. Other communication infrastructures, such as intercom systems, which use other protocols in addition to SIP, are connected in the conventional way.

Firewall

The SBC does not provide firewall functionality and is therefore an extra system requirement. The firewall prevents unauthorized external access and protects the IDDS UCiP system from malicious, unauthorized and faulty connections or packets. There is one firewall cluster for each control center/technical node with IP telephony connection. Pre-existing firewall clusters can also be used and extended.

eurofunk Emergency and Telephone Gateway (ETGA)

The eurofunk ETGA processes external VoIP connections and makes them available to IDDS UCiP users in the usual way. →

To facilitate the emergency call connection, the network operator specifies and supplies the remote devices required for the network. Network operators offer three different connection types for implementing IP emergency calls:

- **Type 1:** Connection without multipath routing
- **Type 2:** Connection with edge-disjointed multipath routing
- **Type 3:** Connection with node-disjointed and, by definition, also edge-disjointed multipath routing

In our opinion, only type 3 is suitable for medium and larger scale control centers because only they have the necessary redundancy.

How Type 3 works:

Separate emergency call routing is always provided over fiber by the network operator. The two paths operate in active/backup mode and are never used simultaneously. This is handled by the Virtual Router Redundancy Protocol (VRRP). In the event of a switchover, only the IP transport path is changed. The SIP endpoint in the telecom network remains the same. Any calls that are in progress at the time are not affected by the switchover.

eurofunk always provides component redundancy for the SBC, firewall, ETGA and network (switch/router) as standard for the connection. This ensures that there is no single point of failure in the eurofunk system.

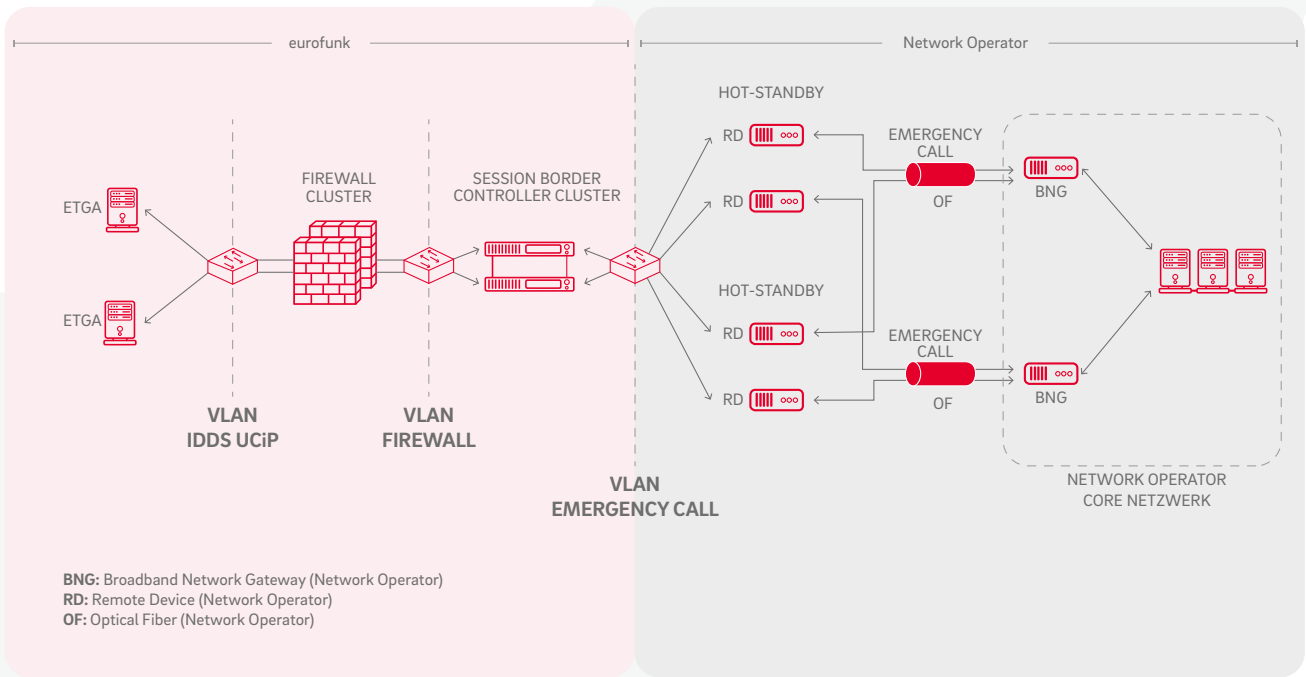


Fig. 1: Type 3 Emergency Call Connection – An emergency call with a fully redundant connection



This means that at least two ETGAs are always included. Depending on the number of SIP trunks or channels per SIP trunk to be connected, more than two ETGAs may be required.

Current Development Status and Outlook

Feature development and expansion to include IP telephony is divided into several phases, the first of which deals with the functional requirements for IP emergency call integration. This first phase covered implementation of the basic functional requirements and full IP emergency call connectivity. In 2019, joint tests were carried out with network operators. The first pilot systems at customer sites were scheduled to go live in the first half of 2020. From the release onwards, all interested existing customers can use these functions through a system extension of IDDS UCiP.

Later phases will also include broadband services in accordance with the German **Technical Guidelines for Emergency Calls 2.0, Federal Network Agency 2018**. These have yet to be standardized and made available.

We are happy assist with your hardware preparations (SBC, firewall, network and virtualization platform) and to draw up an implementation plan with you.

Digital Radio Connection in Germany – Gateway at the DXT Location

Digital radio has been a mainstay of BOS emergency response organizations in the Federal Republic of Germany for some time. Even in an age of increasing digitization, verbal communication is still crucial in times of crisis and emergency. Secure communication over digital networks between emergency personnel and control center remains a key factor in maintaining control of critical situations and for handling emergencies efficiently.

There are numerous solutions on the market for connecting control centers to the BDBOS-TETRA digital radio network and no easy way to know which is the right one. In many cases, the decision is heavily influenced by implementation costs. In others, it depends on the requirements and the existing infrastructure, which in turn result in a number of different possible connection solutions.

There are also different types of wired connections. In addition to the classic connection model (LS1, LS2), solutions involving concentrator gateways or digital radio connectors can also be considered. Each type has its own advantages and disadvantages.

In the original LS1 and LS2 classic connection model, speech is transmitted using expensive E1 lines. This solution is no longer actively offered by network operators and is scheduled for complete withdrawal in the medium term.

With a concentrator gateway connection, the gateway picks up the E1 connection and „bundles“ the speech into VoIP packets that are transmitted to the control centers over IP lines. The speech content remains unchanged; it is merely transported differently - as an IP packet. This connection type requires the addition of a concentrator gateway component to the system. A similar approach is used for connection via a digital radio connector gateway. As well as transmitting speech in IP packets, voice data is decrypted according to German BSI standards and transcoded according to G.711. In addition, the control information and encryption of the data content (e.g. text SDS or location

data) are transferred to another protocol. As with the concentrator gateway solution, the digital radio connector is an additional system component.

In our opinion, the ideal solution for connection to the TETRA network is to combine the advantages of all these connection types. eurofunk has developed just such a solution, working in close cooperation with the German state of Schleswig-Holstein. The solution, which has already gone live at the Western District Control Center (municipality and police), uses the TETRA Gateway (TeGa) at the DXT location, developed by eurofunk. The TETRA gateway handles encryption and decryption according to German BSI standards, it transcodes voice data according to G.711 and bundles the IP packets for audio. The resulting benefits are an IP connection between the control center and DXT (Digital Exchange for TETRA), reduced complexity and the elimination of the need for additional components in the system.

The TETRA gateway at the DXT location is even more interesting for control centers that are linked together to form a eurofunk control center network. The integrated approach and flexibility provided by IP-based routing mean that a technical node can be set up at the DXT location. As a result, TETRA resources can be easily distributed to various locations, promoting cross-team collaboration.

This approach also minimizes the risk of a component or feeder route failure as a node can be very easily set up using redundant IP lines.



Harald VIEHAUSER

Looking at the factors **simplicity, maintainability, availability** and above all **cost savings**, the question „Which connection to digital radio is the best?“ can be answered very simply: „eurofunk TETRA Gateway (TeGa) at the DXT location“.

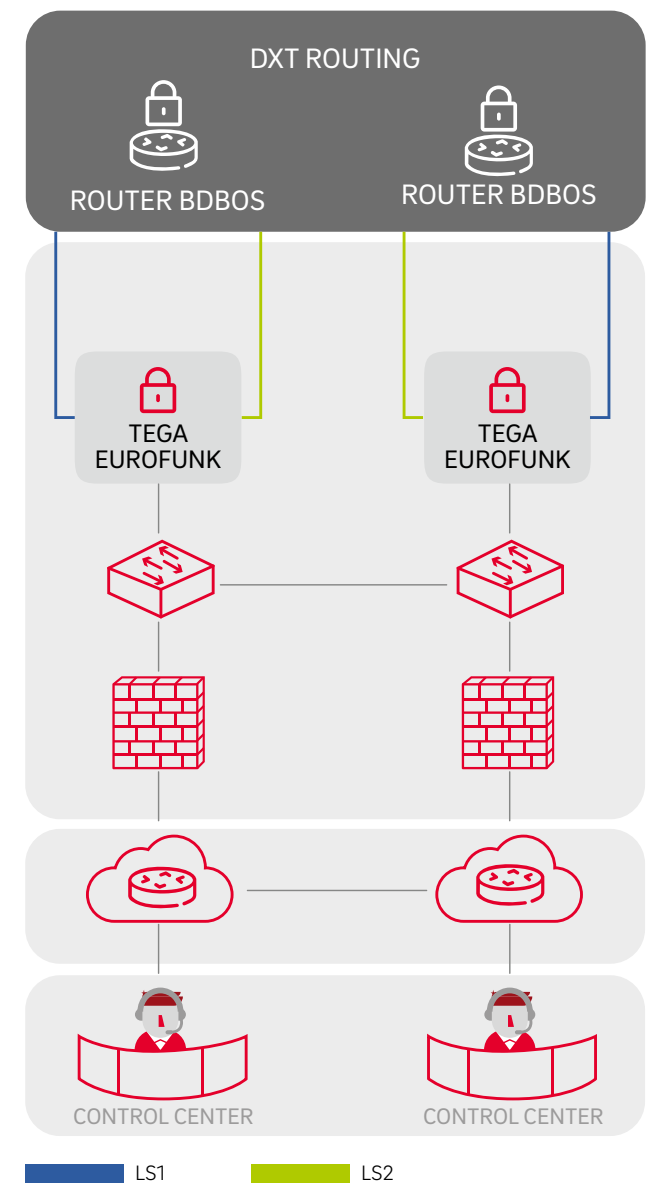
Advantages of the eurofunk TETRA Gateway (TeGa) at the DXT Location

- In comparison with the classic connection model (LS1, LS2): The need for an elaborate and costly E1 connection between the DXT and the control center is eliminated since conversion of speech to VoIP takes place at the exchange and is then transmitted over IP networks. The same IP connection is also used for data transmission.

- In comparison with a concentrator gateway: No additional gateways are required for transcoding speech, such as a concentrator gateway or digital radio connector gateway, as this task is already performed by the TETRA gateway. This means that there are no extra costs for additional components.

- In comparison with a digital radio connector gateway: By reducing the number of components, the degree of complexity is also reduced. This in turn facilitates fault analysis and simplifies maintenance and service responsibilities since there is no dependence on third-party suppliers for concentrator or digital radio connector gateways.

- Maximum availability can be achieved by locating TETRA gateways at two or more DXT sites (redundancy) and combining this advantage with usage by multiple control centers (cost savings).



emc^{WEB} – the new, web-based member of the emc² VOIP communication solution family

eurofunk has always responded to the constantly growing requirements of our customers with the most flexible system design solutions possible. Our mission is to provide a platform for control centers which meets current and future technical requirements. A georedundant system architecture helps control centers to meet the demands of their operational obligations. The most modern, appropriate and optimized technologies are employed here.

The emc² VOIP family of systems has met this demand since its launch in 2005. With the addition of a full WEB extension to our communications solution, we have set a new benchmark in the use of state-of-the-art technology. In addition to the many well-

known benefits of the emc² family, emc^{WEB} now offers a host of new advantages.

emc^{WEB} advantages at a glance:

- Workstation virtualization
- Platform independence
- Full web browser functionality with the ability to use devices, e.g. tablet, in parallel or independently
- Compatibility with MediaServer2 or higher generation systems (full investment protection for existing customers)

For operators of control centers, these advantages offer an even simpler and more cost-effective way of setting up support and redundancy scenarios, by using their own backup sites or other locations within the group network. The usual tried and tested networking options are available. Remote workstations can be integrated with minimal effort and role management is already an integral part of the WEB extension.

The emc² VOIP communication solution WEB extension is currently in the implementation phase of a pilot project involving 26 emc^{WEB} workstations. The complete product rollout and market launch is scheduled for Q1/2020.



Fig. 1: Exemplary representation of an incoming emergency call

We look forward to discussing the application possibilities for your control center environment. Why not contact us?



Peter KLIX

Automatic triggering of digital radio alerting in control centers

The federal states of Hesse and Bavaria have pioneered the use of the TETRA digital radio network for alerting emergency services. The first stage was to develop a technical concept for digital alerting using the existing TETRA digital radio network in Bavaria. The detailed specification and parameters were developed by a project group consisting of representatives of the Bavarian Ministry of the Interior, Sport and Integration, the DigiNet project group and operators of integrated control centers. The existing systems were then upgraded, and large-scale tests carried out in pilot control centers.

The alert process in integrated control centers is normally handled by the incident management system. Redundant TETRA gateways on the eurofunk IDDS communication platform provide the data connection with the TETRA

network through a wired connection. If a gateway fails, redundant gateways take over all operations. If the TETRA gateways or the wired connection to the DXT location are not available, the existing FRT (Fixed Radio Terminal) fallback level can be used. This assures a high degree of availability for both alerting and normal operations.

However, redundancy requirements for integrated control centers also include alerting for an emergency operating level when the incident management system is unavailable; it is designed to be operated both as a stand-alone solution and as an application which is integrated into the existing communication client. The redundant TETRA gateways are used to connect to the TETRA network over wire. If the wired connection fails, the FRT fallback level can be used.

This solution makes it possible to transfer the relevant alert data stored in the incident management system, thereby minimizing maintenance requirements. Alert settings are displayed as buttons in the user interface and can be selected according to alert type or searched for using a simple search facility. The solution's emergency operating level also allows for the manual entry of text messages or the selection of message templates. After the alert has been triggered, the current alert status is displayed. A log is also available for review purposes.

In summary, all essential system components are provided to enable control centers to use digital radio to alert emergency services in real time. The commonplace usage of analog 5-tone alerting should soon be a thing of the past.



Fig. 1: Illustration of an Emergency Operating Level – Main screen



Christian HUBER

Dispatch Center Interface

STANDARDIZED COLLABORATION ACROSS SYSTEM BOUNDARIES.

Control centers are frequently confronted with situations which require close cooperation with external organizations and other control centers in order to handle incidents as quickly and efficiently as possible. Parties involved may have different operational or territorial responsibilities. This is particularly true in areas adjacent to jurisdictional boundaries where it may become necessary to deviate from usual standard processes. Such circumstances might include, for example, cross-boundary emergency rescue and patient transport management or large-scale, cross-border disaster scenarios.

In addition to local cooperation in border regions, situations requiring collaboration may arise among organizations operating within the same territory. Infrastructure, geography and other factors can have a decisive impact here on the level of collaboration required.

Despite incident details being captured and recorded in an incident management system, external organizations and partner control centers are often kept informed by telephone or fax. Although well-intentioned, this break in the medial process often affects standard workflow processes resulting in, for example, the double input of incident details and a subsequent delay in the alerting of resources.

With advances in the networking of IT system environments in the German BOS (Authorities and Organizations with Security tasks) region and the increase in national and international collaboration for incident handling, the demand for software-based solutions to support such cross-organizational cooperation is on the rise. In addition to technical requirements, organizational frameworks must also be considered, since both incident/event handling and tactics can vary between control centers and organizations.

EU-funded Standard Protocol

One approach to standardizing incident-based cooperation has been developed by the EU-funded INTERREG project **Data Exchange between Control Centers**¹. Working in tandem with the

Salzburg Red Cross, Control Center Tyrol and the Free State of Bavaria, eurofunk was one of three companies involved in the project implementation stage. The aim was to create a European-sponsored standard protocol for cooperation across control centers. The protocol sets out the technical specification for communication interfaces between incident management systems on the one hand and regulates the bilateral coordination necessary for cooperation between the respective communication partners on the other.

The key objectives here were the preservation of control center autonomy as part of the internal process design, bilateral freedom of communication and communication coverage between control centers where regional and functional responsibilities differ.

The development of the Dispatch Center Interface (DCI), which provides additional functionality to the incident management system, was a direct outcome of this project. It fulfills three essential tasks:

- An interface to the mission control system providing processing capabilities to support DCI workflows (messaging and controls)
- Information mapping for the implementation of a broad range of codes (bilateral coordination)
- Management of communication tasks between incident management systems (message interface)

The DCI standard defines baseline procedures and message content to best reflect potential cooperation scenarios. These include:

- Event forwarding
- The request of resources for support
- Resource or master data synchronization

In addition to core process messaging, DCI provides other types of telegrams such as event updates and resource status changes. Queries have also been developed for the periodic status monitoring of DCI remote sites and reporting of subsequent interface failures. Furthermore, when a system connection to a



Matthias DOPPELMAYER

DCI communication partner is first set up, the capabilities of the system are queried using DCI methods. This provides an overview of the cooperation scenarios possible with a given DCI remote site.

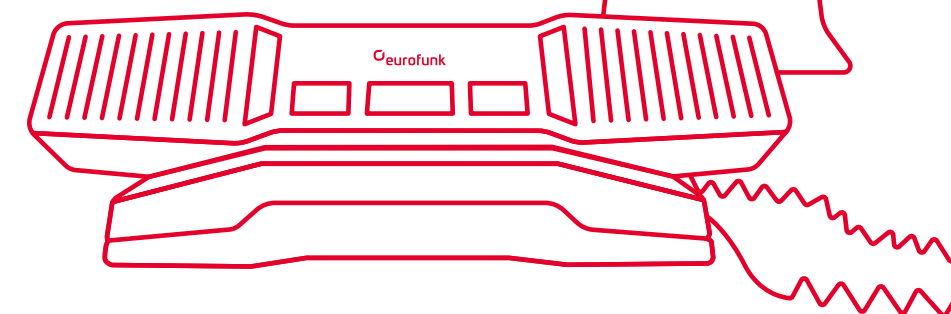
Interface communication

Data exchange over the network can be via a point-to-point connection or VPN (Internet, encrypted). As a rule, communication partners are directly connected to each other. In the case of a control center network, where separately located control centers are linked together, gateways can be used to secure individual transmission paths. The communication interface is defined as a web service (WSDL, SOAP) and accessed over HTTPS.

Inclusion in eurofunk's ELDIS 3 incident management system

DCI has been included in the ELDIS 3 incident management system product portfolio as the standard for bi-directional control center collaboration. Technical design options can be tailored to individual customer requirements.

ELDIS 3



¹ www.dispatchcenterinterface.eu

Ergonomics – what is our vision of the future?

Meet the workplace challenges of tomorrow with the highly customizable eurofunk eDESK including the myDESK application!

Ergonomics describes the relationship between people and their working conditions. If your goal is to have efficient, healthy employees, an ergonomic workplace becomes a prerequisite. This includes factors such as correct posture while standing and sitting, the positioning of input devices and screens as well as optimum workplace lighting – all of which have been shown to have a strong impact on concentration. Should the design surrounding these aspects turn out to be unfavorable it can affect work quality negatively and result in fatigue and a loss of efficiency.

>> It is our mission to understand distinctive human characteristics, abilities and limits and to consider these in the ergonomic design of our products! <<

What role will ergonomics play in the working world of the future?

Rapid technological progress and the associated increase in system functionalities present undeniable challenges. The more information a person receives for processing, the more responsibility he must assume. Overwork, lack of concentration, an inability to handle difficult situations and a susceptibility to errors could result from this additional strain. Concentration on the human aspect is therefore paramount to future considerations. The relationship between people and the workplace should result in a symbiotic community. Workplace design must take individual and personal needs into account and ensure that every interaction becomes a pleasant experience.

A study¹ on the workplace of the future by IDG Research, a leader in the fields of technology, media, data and service, has found that work environment and the ability to make decisions on workspace setup are perceived as areas most in need of improvement in future workplace design. 39.5% of research participants felt that an agreeable environment and better ergonomics would have a strong influence on their choice of workplace. Based on these statistics, it behooves employers in times of labor shortages and high fluctuation to invest in the health and performance of their employees.

These and other considerations have shaped the design of the eDESK family of products, of which our desk generation for control centers is an integral part.

eurofunk eDESK - user-oriented design

The eDESK product family is a perfect combination of simple, elegant design and intuitive handling. True to the motto „design meets technology“, individual components have been united to create a complete mission control system with a balance of virtual and actual workplaces. The consistent implementation of the „clear desk“ principle has helped us free the space of unnecessary distractions, thereby reducing psychological stress and increasing concentration levels.

Added to the current – indispensable – feature of adjustable work surface and monitor heights, which allows for individual sitting and standing positions, the eDESK offers further improvements and possibilities for customization.

A good example of this is the dynamic lighting provided by the eurofunk Light & Sound Bar. Designed to imitate natural lighting as it relates to our internal clock, the Light & Sound Bar makes it possible to regulate both light intensity and color temperature. Control elements for this were added to the eDESK touch pad with strict adherence to the „clear desk“ principle. The simple and direct touch of the keys embedded in a flush-mounted capacitive keypad helps the operator to adapt the workspace without losing focus on the essentials.

Stepping just a little further into the future we can choose to leave the touch control elements where they are and adjust our work stations using gestures. Yes ... gestures! The eDESK gives you the option to configure a gesture-controlled integration. Using a defined combination of simple and intuitive hand moti-

¹ www.arbeitsplatzderzukunft.de/wp-content/uploads/IDG-Studie_Arbeitsplatz-der-Zukunft_2018.pdf



the new eDESKc with the eBOX

ons, it is possible to place the entire workplace control – quite literally – in the hands of the user.

eDESKc

With the eDESKc we no longer speak of visions but of realities – realities in which control center workstations are provided with the synergies necessary to make human-machine interactions all but seamless.

The idea behind the eDESKc model was to produce a more compact version of the eDESK while remaining true to product identity. The eDESKc is available as an entry-level model in the eDESK family and offers the functional configurations popular in the main model.

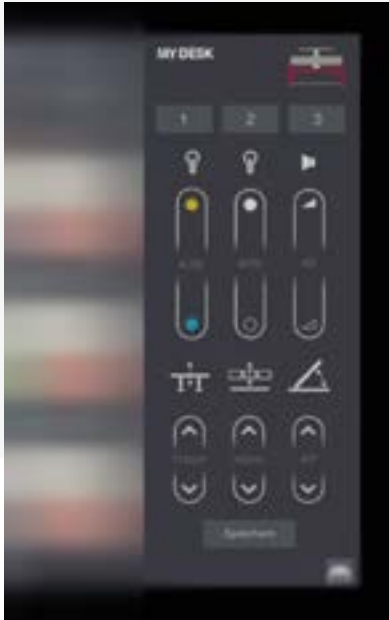
Also reflected in the eDESKc is the eDESK philosophy. In addition to the same high-quality material selection and the use of innovative elements (e.g. Light & Sound Bar), the entry-level model also considers the haptic separation between the palm rest, work surface and touch input area. Here, too, the user has access to a completely new eDESK experience!

Setting itself apart from the rest of the product family is the compact, vertical drawer system we call the eBOX. The eBOX can be integrated on either side of the workstation and guarantees complete flexibility in design. Here you will find a suitable place for personal items such as cell phones or documents which helps to keep the work surface tidy and free of clutter. The pull-outs are equipped with LED interior lighting and USB ports and can be used for things like charging mobile devices. →

ERGONOMICS



Daniele TAGLIANI



Design, ergonomics, innovation:
we call it the eDESK experience!

myDESK - The workplace application

The eurofunk myDESK application integrated in the eOCS (eurofunk Operation Center Suite) mission control system allows you to personalize your work station and save your preferred settings.

Operators then can load their personalised eDESK settings and dynamically adapt their workstation to their own requirements.

Overview of myDESK functionalities:

- Adjustment of the desk height incl. display in cm
- Adjustment of the monitor height incl. display in cm
- Adjustment of the touch screen tilt incl. display in degrees
- Regulation of light intensity (Light & Sound Bar) incl. display in percent
- Regulation of the color temperature (Light & Sound Bar) incl. display in Kelvin
- Control of status display (Light & Sound Bar) according to defined states (e.g. operator needs assistance)
- Individual storage and configuration of multiple user profiles



eDESK debut in Salzburg

Well-known for their modern, progressive outlook, the Salzburg Professional Fire Department was, once again, first to embrace our innovative workplace design. In May of this year eurofunk completed the installation of five eDESKs.

The set-up consists of three uniformly designed eDESK (ELP1-3), combined by elegant 45-degree connecting elements that form a command center by bringing the harmonious form of the workstations together. Slightly offset but nicely integrated into the room, one additional eDESK (ELP4) is configured for the role of shift supervisor.

To complete the room design, we added an eDESK straight (ELP5) to act as fallback and a central conference table in matching design.

If you would like to learn more about the eDESK product family, ask for our eDESK brochure. We would be happy help you design your control center of the future!

A control center deputizes for itself - Modernization at ILS Nuremberg

In an era of technological innovation and ever-changing requirements, operators of critical infrastructures are continually striving to keep their equipment up to date. To this end, the Integrated Control Center in Nuremberg (ILS Nuremberg) made the decision to modernize its control center infrastructure in the summer of 2018

The project's scope, which entailed reconstruction, renewal and an increase in functionality at one of the largest fire and rescue control centers in Germany, was akin to open-heart surgery. It was clear to the entire project team, that day-to-day operations, unrestricted availability, the high standard of emergency call handling and incident processing could not be compromised at any time during the modernization process.

Meticulous planning over several months in close consultation with ILS Nuremberg and the technical planner, paved the way for a successful project implementation phase. Rigorous testing of mission-critical interfaces was also undertaken ahead of migration.

The Integrated Control Center's own relief control center, Emergency ILS, was to play a central role in the reconstruction by taking over full control of control center operations for a period of three weeks. For this to happen, it was equipped with the latest technology and 16 mobile workstations, complete with furniture.

The modernization of ILS Nuremberg comprised the renewal of IT and communications technology as well as the following additional functionality:

- Replacement of the IDDS-512 communication system with the IP-based **IDDS UCiP** system
- Addition of a redundant, wired digital radio connection
- Equipping of the Emergency ILS with **emc²VOIP** as a fallback level for communications
- Provision of an application cluster with a high level of redundancy (Oracle-RAC) for the incident management system
- Import of the latest communication system and incident management system software version

A point worth emphasizing is that now, all regular and emergency control center workstations in the network can be used in parallel (e.g. in special operational situations or for training purposes).

It is thanks to the close cooperation between ILS Nuremberg and eurofunk, that the objectives - especially regarding availability and adherence to schedules - were met throughout the course of the project.

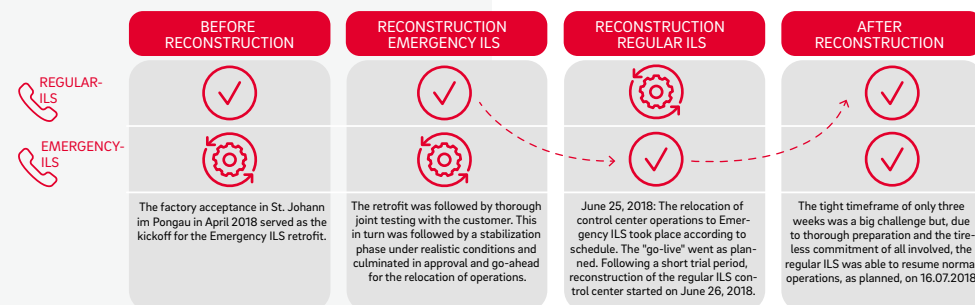


Fig. 1: Migration Timeline

ILS Nuremberg: Facts & Figures

ILS Nuremberg is one of the largest control centers for fire and rescue in Germany. It provides support for:

- The cities of Nuremberg, Fürth and Erlangen as well as for the rural districts of Nuremberg Land, Fürth and Erlangen-Höchstadt
- An area covering over 2,000 square kilometers
- Approx. 1.2 million inhabitants

Annually they handle:

- Around 700,000 calls, of which 243,000 are 112 emergency calls
- Over 290,000 deployments consisting of:
 - Fire service 17,500
 - Emergency response 164,500
 - Patient transport 111,500
- 236,000 enquiries not requiring a resource response

To deal with these volumes the Integrated Control Center (ILS) has:

- 16 fully-equipped workstations + 3 in procurement
- 10 additional workstations for handling emergency situations
- 6 workstations at the fire station control center
- 16 backup workstations at the Emergency ILS control center



Johann FRITZ



Current Outlook:

ILS Nuremberg has commissioned eurofunk to increase its capacity and efficiency in response to the steadily increasing number of emergency calls and incidents.

In the coming months, we will be delivering three more fully-equipped workstations as well as ACD (Automatic Call Distribution) call center technology. In addition, the current eCall solution will become part of the fully integrated eurofunk solution.

We are already looking forward to the next stage in this successful working relationship!

eurofunk Automatic Call Distribution



Günter DUTZLER

Fast, efficient and reliable emergency call handling lies at the heart of control center operations. With the telephone remaining the primary means of communication between caller and control center, eurofunk's main drive, as communications system provider, has been to improve the quality of emergency call management by planning and developing new features for its communication solutions. One such addition is the **eurofunk Automatic Call Distribution (ACD)** feature.

eurofunk ACD differs considerably from ACD systems commonly used by call centers and hotlines. Adapted to the specific needs of the emergency services, however, Automatic Call Distribution is a powerful tool that reduces peripheral noise and the stress that comes with constant decision making.

Let us run you through some of the most important functionalities offered by the eurofunk ACD solution:

In standard ACD systems incoming calls are only announced to available workstations. If all workstations are busy, the call is not announced but held in a queue instead. With this scenario, however, it is impossible to fulfill the emergency call center requirement for rapid call acceptance. Hence, eurofunk ACD takes workstation status (FREE, BUSY or POST PROCESSING) into

consideration and allocates incoming calls to those operators who are authorized and available to take the call. If all workstations are in BUSY mode, the call is escalated, and the emergency call is routed to all operators with one or more roles. After a specified time period, this can be extended to other roles or to all control centers in the network.

One of two allocation rules can be used to determine which workstation receives a call:

Longest idle

If several workstations are free, the workstation that has been free the longest is selected. If no workstations are free, the workstation which has been in POST PROCESSING the longest is selected.

Round robin

If several workstations are free, the next available workstation is selected. After all workstations have accepted an emergency call, the cycle starts again. If no workstation is free, but several are in POST PROCESSING, the next available workstation with this status is selected. The cycle starts again after all workstations have accepted an emergency call.

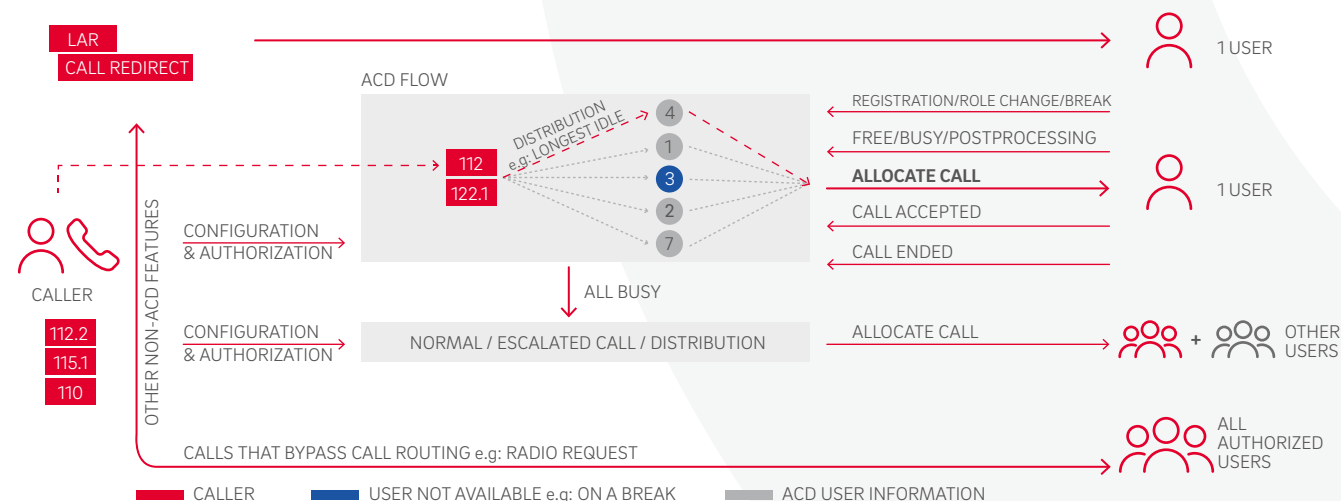


Fig. 1: eurofunk Automatic Call Distribution Flow

eurofunk, your professional partner for implementing the BSI IT baseline protection



York KEYSER

What is the German Federal Office for Information Security (BSI) and the BSI IT Baseline Protection all about?

The Federal Office for Information Security (BSI) was founded in 1991. The German Cyber Security Authority is responsible for prevention, detection and response measures on behalf of the state, the economy and society. It is an acknowledged single point of contact for all information security matters.

The IT Baseline Protection from the BSI provides guidelines which enable authorities and businesses to take protective measures to improve information security. This template is provided to systematically identify and implement appropriate security measures, making the introduction an information security system that much easier.

The introduction of Information Security Management (ISM) is supported by the following standards: 200-1 Management for Information Security, 200-2 IT Basic Protection Methodology, 200-3 Risk Management and 100-4 Emergency Management. The updated Basic Protection includes the IT Basic Protection Compendium. This Compendium comprises modules that cover all common hazards and security requirements which a company faces. The Compendium is updated annually to ensure that it always reflects current circumstances.

BSI IT Basic Protection and eurofunk

Companies have several methods and standards to choose from for achieving their information security goals. eurofunk attaches great importance to two of these standards, the BSI IT Baseline Protection and ISO/IEC 27001 Certification. Whereas ISO/IEC 27001 Certification is internationally recognized and the preferred option for commercial enterprises, the BSI IT Baseline Protection is the information security standard of choice for German public authorities.

eurofunk is matching the security standards of customer systems and extending beyond their long-standing ISO/IEC 27001 Certification. By the end of 2019 all relevant processes, such as customer service operations via remote maintenance, will be certified according to the BSI Baseline Protection.

BSI-IT baseline protection

The IT Basic Protection Compendium describes the requirements or measures that must be taken to secure all areas of the company. This can be achieved, for example, by work instructions or the installation of security software.

The following two examples illustrate how the BSI IT Baseline Protection aims to cover all these areas:

Example 1:
Work instruction from module INF.1 General Buildings

INF.1.A11 Secured doors [Employees]
Employees SHOULD be instructed to lock their office or lock away their paperwork when absent. There SHOULD also be spot checks to ensure that this is being done.



Example 2:
Procedure from the module SYS.2.2.3 Clients with Windows 10

SYS.2.2.3.A5 Protection against Malware
Unless other mitigation measures of equal or greater value have been undertaken to protect the IT system from exposure to malware, a specialized anti-malware component MUST be implemented on Windows 10 clients.



The BSI IT Basic Protection Profile

Many of the measures set out by the BSI IT Baseline Protection are common to all same-sector companies. For this reason, the BSI issued the IT Basic Protection Profile in 2018. This profile, drawn up jointly with industry representatives, can be used as a template by companies in the same industry.

From the outset, eurofunk played an active role in the creation and implementation of the BSI IT Baseline Protection Profile for Control Centers. The profile is intended to assist operators of BOS control centers to implement the requirements laid down in the BSI IT Baseline Protection. The aim is to make the IT and information systems in control centers more secure and to ensure that state-of-the-art security standards are maintained at all times.

At the end of June 2019, eurofunk jointly organized a kick-off workshop with the BSI and industry representatives to create this profile. The kick-off workshop will be followed by two further dates aimed at finalizing the BSI IT Baseline Protection Profile.

The profile will be published by the BSI on completion. Once this has been done, our customers will be able to implement the BSI IT Baseline Protection more quickly and easily, knowing they can rely on eurofunk expertise and support.



Greenbone

The BSI IT Baseline Protection alone is not enough; the IT Baseline Protection Compendium makes repeated reference to penetration testing and vulnerability analysis for just this reason. eurofunk has used a vulnerability scanner to monitor continuously its own internal systems for some time now. An additional scanner has been used since the beginning of 2019 to improve security in customer projects as well.

This type of scanner is used to scan a system or an entire network for known vulnerabilities. The scanner can perform close to 70,000 automated scans. The vulnerability scanner attempts to log into a variety of different systems, checking both standard usernames and passwords. It also checks the software installed on the system for vulnerabilities. A detailed report highlights the vulnerabilities and provides suggestions on how to fix them.

The large number of scanner providers on the market makes the choice of the right one difficult. eurofunk finally opted for Greenbone. This provider has been on the BSI recommended list for several years. An added advantage is that a German license is already available for our customer to use.

More and more customers are turning to a vulnerability scanner as a means of providing the best possible protection for their systems.

We are happy to support your needs with our Greenbone vulnerability scanner!

NEWS, the client magazine of eurofunk KAPPACHER GmbH, is published once a year.

**Media Owner (Publisher),
Published and edited by:**
eurofunk KAPPACHER GmbH
eurofunk-Straße 1 – 8
5600 St. Johann im Pongau
Österreich / Austria
office@eurofunk.com

Content:
CEO Christian Kappacher,
Dr. Christian Kappacher

Liability:
The publisher, authors and editors shall not be held liable for the content of NEWS, the correctness of the information or any errors.

Images:
Adobe Stock
Christoph Hettegger
ILS Nuremberg
Lorenz Masser

Published and produced in:
St. Johann im Pongau

www.eurofunk.com





eurofunk

creating safety by technology



eurofunk KAPPACHER GmbH
eurofunk-Straße 1–8
5600 St. Johann im Pongau
Österreich / Austria
T +43 57 112 - 0
T +49 7231 7782 - 0
office@eurofunk.com
www.eurofunk.com

