SPLOŠNA BOLNIŠNICA SLOVENJ GRADEC

GOOD PRACTICE

Modern network infrastructure for efficient digital management and increased patient satisfaction at Slovenj Gradec General Hospital

Using the Extreme Networks equipment, in cooperation with our partners Kopa d.d. and Smart Com d.o.o., we have taken the institution's network services to an entirely new and significantly higher level.

Branko Knez
IT Department, Slovenj Gradec General Hospital

Foto: Doris Kordić

SMART COM

Extreme networks

Technology partner

About Slovenj Gradec Hospital

Slovenj Gradec General Hospital is the main secondary-level health care institution in the region of Koroška, providing its citizens with high-quality, safe and comprehensive healthcare services.

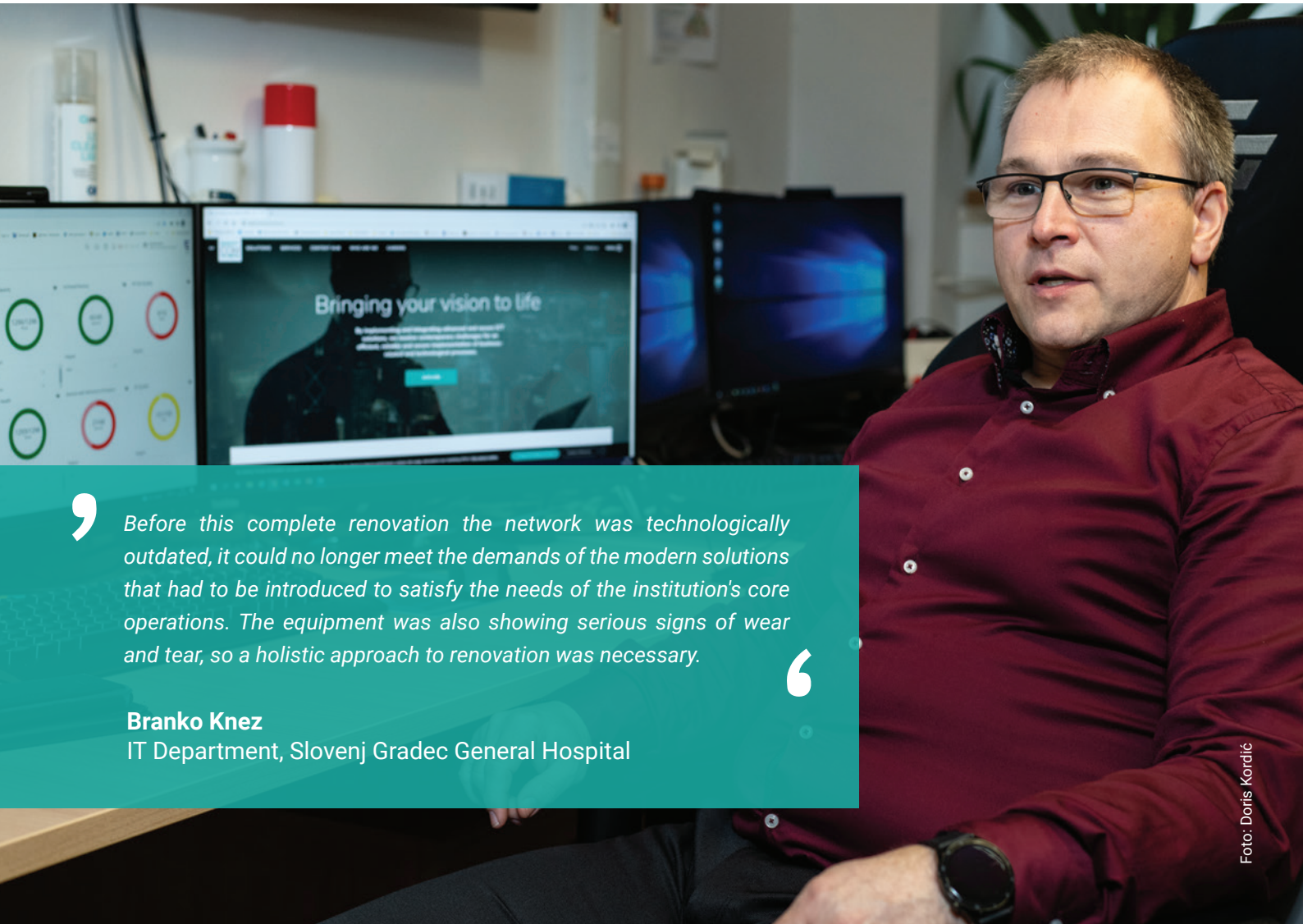
The hospital's mission is to provide quality healthcare services and make sure these services are accessible to all. Its main objective is a cured and satisfied patient.

Achieving this vision involves setting ambitious goals, including digitalisation and automation. These technological trends, together with innovations, are the drivers of development and competitiveness that will further contribute to the ultimate goal of better healthcare.

And improve work processes and working conditions for healthcare staff.

Digitalisation must go hand in hand with the introduction of modern telecommunication solutions and with ensuring a reliable, stable and secure IT environment in the hospital.

Therefore, in recent years, **the existing infrastructure has been renewed and upgraded by modernising the LAN network** and establishing or extending the wireless network.



Before this complete renovation the network was technologically outdated, it could no longer meet the demands of the modern solutions that had to be introduced to satisfy the needs of the institution's core operations. The equipment was also showing serious signs of wear and tear, so a holistic approach to renovation was necessary.

Branko Knez
IT Department, Slovenj Gradec General Hospital

Foto: Doris Kordić

The Challenges

The increasing complexity of modern business, technological change – the increasing number of applications, the introduction of advanced technologies such as telemedicine, IoT devices, digitisation and robotics – are changing the way healthcare institutions operate.

All this requires a reliable, flexible and secure network infrastructure that can respond to the demands of modern healthcare models, including by enabling secure mobility of healthcare professionals and staff in their local network and providing secure internet access to all others, including visitors.

The building blocks of the hospital's existing LAN were technologically outdated and did not provide a sufficient level of security and user mobility. Given that the demand for mobility and consequently wireless connectivity is growing rapidly, and that prior to the renovation, adequate wireless coverage was only provided in the newly built C1 block and the fully renovated C2 block, which is only a quarter of the institution, this represented an additional reason for the renovation.

Therefore, in cooperation with the partners Kopa d.o.o. and the experts of the system integrator Smart Com d.o.o., in addition to a complete overhaul of the LAN network, fire barriers and secure remote access for employees and partners, a secure wireless access to the LAN network was established, enabling provide wireless access for employees as well as for guests or business partners. At the same time, a high level of security has been ensured.

An innovative solution

When designing the entire network we were guided by the requirements for high service availability and business continuity.

The decision was made to deploy state-of-the-art solutions from Extreme Networks, which provide a high-performance, reliable, yet flexible and upgradable network.

Depending on the requirements, the user communication hubs were designed with double-wired network switch stacks. In addition to higher data throughput, this ensures a higher level of network reliability and security.

Integrated components from the technology provider Extreme Networks:

1. core aggregation server switches and data centre switches,
2. user access switches,
3. central wireless device, and
4. the ExtremeCloud IQ control system.

The network segmentation, which is enabled by the advanced network design, provides greater security, and **the integrated switches provide protection against commonly used types of cyber-attacks**, such as DoS attacks, DHCP snooping, etc., which can cause poor server responsiveness and thus the non-functioning of individual applications.

A two-tier network topology is applied, implemented using the MLAG (*Multichassis Link Aggregation*) technology, which **allows for high reliability, throughput and availability of the network**. This means that when a link

between hubs fails or a core switch fails, the outage is not felt by the users.

The integrated equipment also has the advantage of **unified software on the core networks**, the data centre and the user hubs. The software itself is modular, which means that in the event of a failure of e.g. the SNMP protocol, SSH or routing, the uninterrupted operation of these protocols can be ensured by restarting the individual software module without the need to restart the individual device.

At the edge of the network, secure and controlled connection of users is ensured with the help of the NAC (*Network Access Control*) functionality, which allows to define groups of users according to several parameters (authentication type, MAC address, subscriber, location, time of connection, etc.), the NAC then recognises the user and, according to the defined rules, automatically places them in the right group (with the appropriate access rights) or in the appropriate VLAN, regardless of which switch they are connected to.

The network paves the way for hospital digitisation and robotics

Digitalisation brings many benefits that improve working conditions and safety in the workplace, ultimately affecting patient care and satisfaction. That is why Slovenj Gradec General Hospital has set itself the extremely ambitious goal of **setting up an autonomous transport system – the ATS GoCart 250 for the transport of pharmaceutical materials**. The system was developed in cooperation with the hospital's partners *Viptronik d.o.o., Sumetzberger GmbH, and Yujin Robot Co. Ltd.*

Reliable network connectivity (in all its forms, both wired and wireless) is essential for this innovative solution to work effectively. Connections between dedicated servers, lift controllers, access controllers, automatic door openers, fire alarm control centres, etc., are wired into the network through various communication hubs throughout the facility. The control panels with user interfaces, which serve the interaction of users with the ATS system, are connected to the wireless network. Similarly, the two AMR (*Autonomous Mobile Robot*) robots, which are part of the ATS system, use wireless network connection for simultaneous operation and communication with other technologies.

All communication between all the elements of the ATS system is done in real time using Extreme Networks' state-of-the-art equipment, **ensuring smooth and seamless operation**. This innovative solution has received a lot of attention from healthcare institutions in Slovenia and abroad. It received the Gold Award of the Koroška Chamber of Commerce and Industry and the Silver Award of the Chamber of Commerce and Industry of Slovenia.

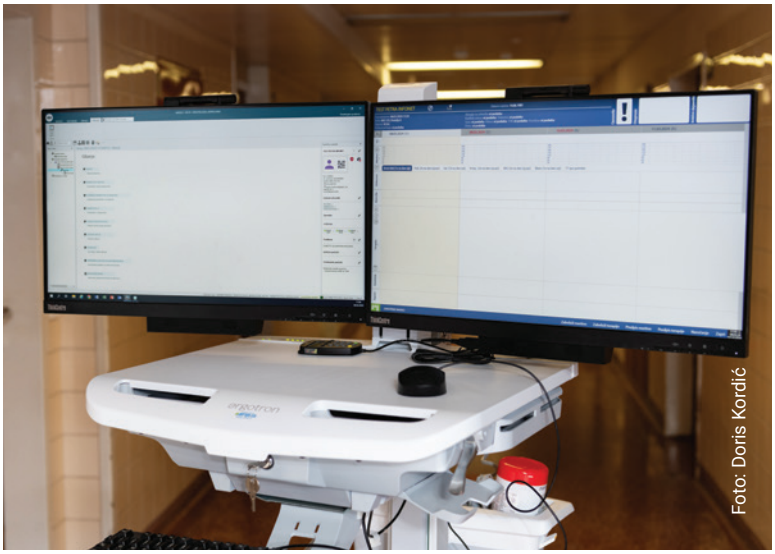


Foto: Doris Kordič

Another high-profile project has been implemented where, in addition to the solution itself, the infrastructure supporting digital patient care at the bedside is also very important. An **electronic temperature and therapeutic sheet service** – eTTL – was implemented throughout the facility. The introduction of this new paperless solution has completely transformed and digitised the process of conducting rounds. Dedicated solutions have been developed to meet the needs of this service, tailored to the specific needs of the two groups of professionals – doctors and nurses. The solution includes dedicated mobile units equipped with laptops or AIO computers with one or even two 24" displays. The mobile units, connected to a wireless network, are moved around the ward

by staff as they carry out their rounds. Because the wireless network allows roaming, employees can use these services continuously and seamlessly across all departments.

Wireless connectivity was also a key response to the challenges of telemetric patient monitoring posed by the COVID-19 pandemic. The requirements for extreme flexibility in terms of being able to easily and quickly move diagnostic devices for monitoring vital signs within hard-to-reach – enclosed – so-called red zones, were successfully addressed without the need to rearrange and reorganise cable connections.

> *With the help of telemetry provider Afiris d.o.o. and the use of the Extreme Networks wireless network, we were able to ensure the monitoring and control of critical patients.*

Branko Knez
IT Department,
Slovenj Gradec General Hospital

Positive impacts

1. The advanced design of the network provides throughput, availability and reliability, fast response times and low latency, making it a good foundation for technologies such as IP telephony, video conferencing and other demanding applications.
2. Phased expansion and management of wireless hotspots is possible.
3. The network enables easy creation of a new hub and connection of users without the need to further identify and add VLANs per port for each user.
4. Unified control and management of network infrastructure (both wired and wireless) from Extreme Networks as well as third-party equipment.

Foto: Doris Kordić

SPLOŠNA
BOLNIŠNICA
SLOVENJ GRADEC

Foto: Doris Kordić

As healthcare providers increasingly rely on digital technologies and interconnected systems, the network is a key component that ensures the confidentiality, integrity, and availability of critical data and services.

In a hospital environment, network security is essential when it comes to networked medical devices and equipment. Ensuring the integrity of these devices significantly contributes to preventing security incidents that could compromise the seamless management of patients.

In order to support the delivery of critical healthcare services, deploy advanced telemedicine services, ensure compliance with relevant regulations and maintain the trust and confidentiality of patients' personal data, it is vital to establish a modern network infrastructure, which represents the basis for conducting business in this digital age.

info@smart-com.si 01 5611 606 www.smart-com.si

SMART COM

Extreme networks

Technology partner