DOI: 10.19279/TVZ.PD.2014-2-2-08

USING SMART GRID TECHNOLOGY IN ENERGY DISTRIBUTION SYSTEMS

Goran Kišan[1], Silvi Kolarić[2], Zoran Baus[3], Dubravko Žigman[4], Krunoslav Rukavina[5], Tihomir Čar[6]

[1]Systems Engineer, IN Time d.o.o. - TNT Global Express
[2]Senior Network Engineer, EagleBurgmann Germany GmbH & Co. KG
[3]Elektrotehnički fakultet Osijek
[4]Tehničko veleučilište u Zagrebu / NetAkademija
[5]Senior Security Analyst, ING Management Services s.r.o.
[6]Networking Consultant & Engineer, Spartacus rješenja j.d.o.o.

Abstract

Using smart grid technology in today energy distribution systems will reduce cost, reach manageability, provide safety of energy supply chain to end customer and provide new innovative energy service delivery.
Term "smart grid" can be explained with following words – intelligent, self-sustained, with management based on IP (Internet Protocol) telecommunication network for transportation of critical data in real-time from customer site (smart meters, smart homes, smart buildings) and distributed power plants to central management station (energy service provider operations). Main function of the central management station is to acquire and evaluate stored data in real time and based on this stored and evaluated data, in case of emergency, power outage on some subsystem or increased need for power on specific location, to apply necessary steps in real-time. Therefore data conformity and security in smart grid technology is an important function concept to implement. Nevertheless primary goal of smart grid technology is to improve the ***efficiency, reliability*** and ***safety*** of power delivery by modernizing both the ***transmission*** and the ***distribution*** grids.
This article has a goal to provide a high-end top-level view of a modern telecommunication infrastructure needed to implement a smart grid technology into an energy transmission and distribution grid.

Key words: *energy distribution systems, smart grid, IP telecommunication networks, real time monitoring and control, data conformity and security*

1. Introduction

Smart grid technology is based on IP transmission network technology (IEEE 802.3, Ethernet, Metro-Ethernet). Such network design solution is based on the principle of service oriented network architecture (SONA) and top -down network design as a hierarchical model. In order to meet above specified preconditions of service oriented network infrastructure, typical network topology design will be based on star or ring topology. Which topology to choose has to be based mainly on cost and other here none specified factors. Technological features of such network are scalability, availability, performance (capacity and speed), manageability, efficiency and security. [1] [2] [3]

This modern technology will use in his access, distribution and core network infrastructure wired (copper and fibre optics) and/or wireless (3.5G and 4G – UMTS, LTE) solutions. In today's terminology smart grid networks are representing a platform based on IP technology which function is to interconnect smart homes, smart connected buildings, utility operations and power plants. To control, measure, monitor and act in real -time there is a substantial computing (server systems) and network infrastructure to build up. We will start with short explanation of server infrastructure and continue with some sentences about network infrastructure. [2]

2. Server network infrastructure for smart grid networks

To control and monitor thousands of smart home energy sensors (based on IP technology), to store and control real-time data from this

in-house sensors is from a computing view heavy-duty task. Under the terms store, control and monitoring is to understand an execution of specialized real-time application programs. This specialized real-time application programs are producing specific data which is saved in databases on storage system infrastructure (billing, accounting). Application servers are using virtual environment operating systems solutions (i.e. Hyper-V or VMware) for high -availability and redundancy in active-active or active-passive clustering configuration.
To reduce high working load of virtualized servers there is a need for implementation of load balancing systems. [2]

3. Network infrastructure and layered system IP topologies: core, distribution, access

3.1 Core Network Layer

The function of network core layer is to provide scalability, high availability and fast convergence. The core layer is the backbone for network connectivity and is the connection point for distribution layer and server application network infrastructure. The core devices implement scalable protocols and technologies, alternate paths, and load balancing. The core layer is designed for scalability and future network growth. Network core is a high-speed Layer 3 routing environment for fast convergence in case of network link or node failure if this scenario could occurs. Network core uses redundant point-to-point Layer 3 interconnections because of the fact of fast convergence. Without a core layer, the distribution layer network elements need to be fully meshed. This type of design can be difficult to scale, and increases the cabling requirements, because each new distribution network element needs full-mesh connectivity to all the distribution network elements. [2], [3]

3.2. Distribution Network Layer

The distribution layer aggregates traffic from all network nodes and uplinks from the access layer. Quality of Service (QoS), load balancing and high availability are the important functions for this layer. High availability is provided through dual paths from distribution layer to the core and from the access layer to the distribution layer. Distribution layer uses a combination of Layer 2 and multilayer switching to segment network regions and isolate network problems inside of them, by preventing the local regional problems to impact the core layer. Distribution layer may be used to terminate VLANs from access layer switches, also distribution layer connects network services to the access layer and implements QoS, security, traffic loading, and routing policies. At last distribution layer can

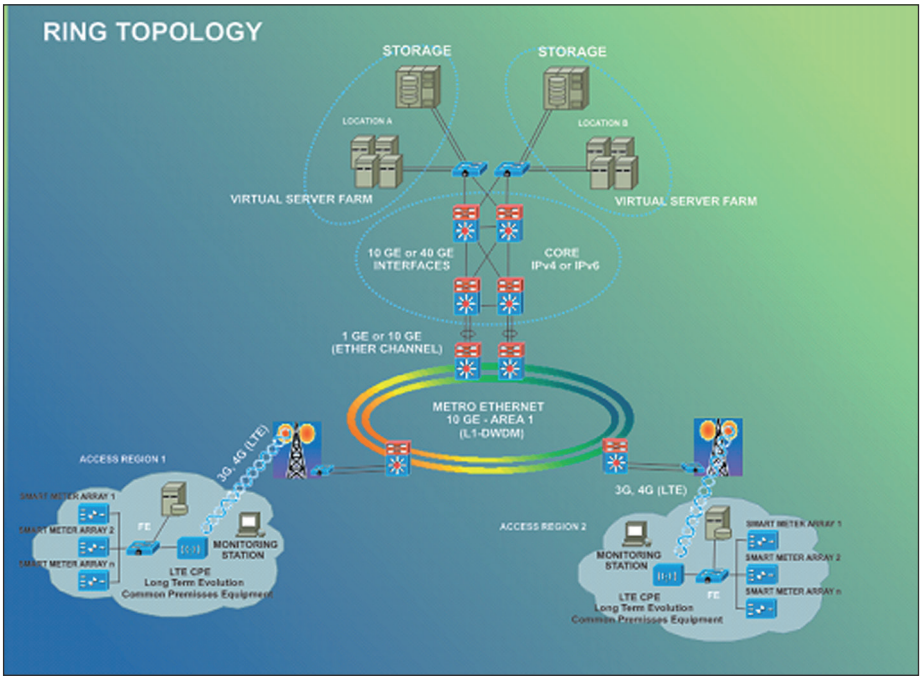

Fig.1 *– Example of ring network topology with implementation of optical ring (DWDM)*

provide default gateway redundancy by using router redundancy protocols (i.e. Gateway Load Balancing Protocol, GLBP or Virtual Router Redundancy Protocol, VRRP). [2], [3]

3.3 Access Network Layer

Access layer aggregates IP access devices and provides uplinks to the distribution layer.
The access layer should support multiple features such as high availability, security and quality of service (QoS). At the access layer, high availability is supported through various hardware and software functions. With hardware, system-level redundancy can be provided using redundant power supplies and redundant uplinks. It can also be provided by default gateway redundancy using dual connections from access switches to redundant distribution layer switches. With software, high availability is supported through the use of first-hop routing protocols, such as Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing Protocol (GLBP). Access layer provides services for additional security against unauthorized access to the network through the use of tools such as IEEE 802.1x, port security, DHCP snooping, Dynamic ARP Inspection (DAI), and IP Source Guard. Access layer allows prioritization of mission-critical network traffic using traffic classification and queuing as close to the ingress of the network as possible. It supports the use of the QoS trust boundary. [2], [3]

4. Network Management

To apply network management strategies there will be two directions – reactive and proactive management strategy. Reactive management is reactive in process, meaning that network administrator/engineer is reacting on specific fault or network event. Proactive management means that that network administrator/engineer proactively checking the health of the network during normal operation to recognize potential problems, optimize performance, and plan upgrades in real-time. Proactive network management is desirable but can require that network management tools and processes be more sophisticated and imply more costs than with reactive network management. [2], [4]

4.1 Types of Network Management

International Organization for Standardization (ISO) defines five types of network management processes (FCAPS): [4]

- **F**ault management,
- **C**onfiguration management,
- **A**ccounting management,
- **P**erformance management,
- **S**ecurity management.

Fault management refers to detecting, isolating, diagnosing, and correcting network problems, it also includes processes for reporting problems to end users and managers.

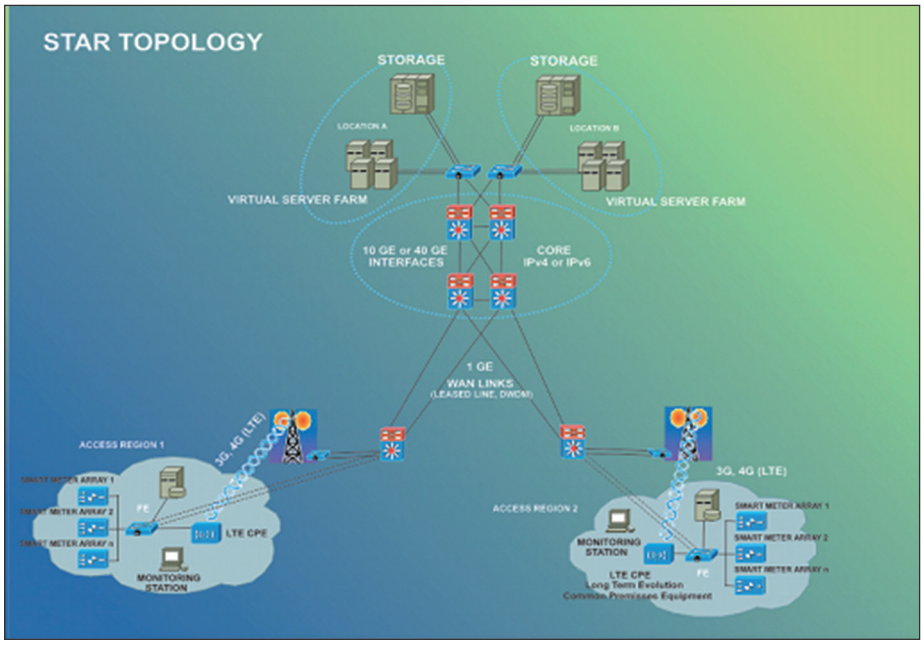

***Fig. 2** - Example of star network topologies with subsystems*

Accounting management facilitates usage-based billing and to track unexpected traffic growth is so that the traffic can be considered during the next capacity-planning phase.

Configuration management helps a network administrator/engineer keep track of network devices and maintain information on how devices are configured and also provides change management.

Performance management includes examining network application and protocol behaviour, analysing reachability, measuring response time, and recording network route changes. Performance management facilitates optimizing a network, meeting service-level agreements (SLA), and planning for expansion. Monitoring performance involves collecting data, processing some or all of the data, displaying the processed data, and archiving some or all of the data. [5]

Security management lets a network administrator/engineer maintain and distribute passwords and other authentication and authorization information. Security management also includes processes for generating, distributing, and storing encryption keys. It can also include tools and reports to analyse a group of router and switch configurations for compliance with site security standards. [5]

4.2 Network Management Architecture

Typical network management system architecture consists of managed devices, agents, and NMSs (Network-Management-System's) computing appliances. There is a two way approach to effective network management: in-band and out-of-band monitoring.

In-band monitoring, network management data travels across network topology using the same paths as data traffic. This makes the network management architecture easy to develop but results in the dilemma that network management data is impacted by problems on the network, making it harder to troubleshoot the problems. [5]

Out-of-band monitoring makes the network design more complex and expensive, because of the fact that there are two deployed networks. Another trade-off with out-of-band monitoring is that there are security risks associated with adding extra links between NMSs and agents. [5]

To ensure high network availability, management tools should support numerous features which can be used for performance, fault, configuration, security, and accounting management. Ideally, the system should also incorporate intelligence to identify trends that can predict a potential failure so that a network administrator/engineer can take action before a fault condition occurs. Monitoring tools are often based on following protocols and standards: Simple Network Management Protocol (SNMP), Remote Monitoring (RMON), Net Flow and Management Information Bases (MIB). [1]

Simple Network Management Protocol (SNMP)

SNMP is supported by most commercial NMSs and many networking devices, including switches,

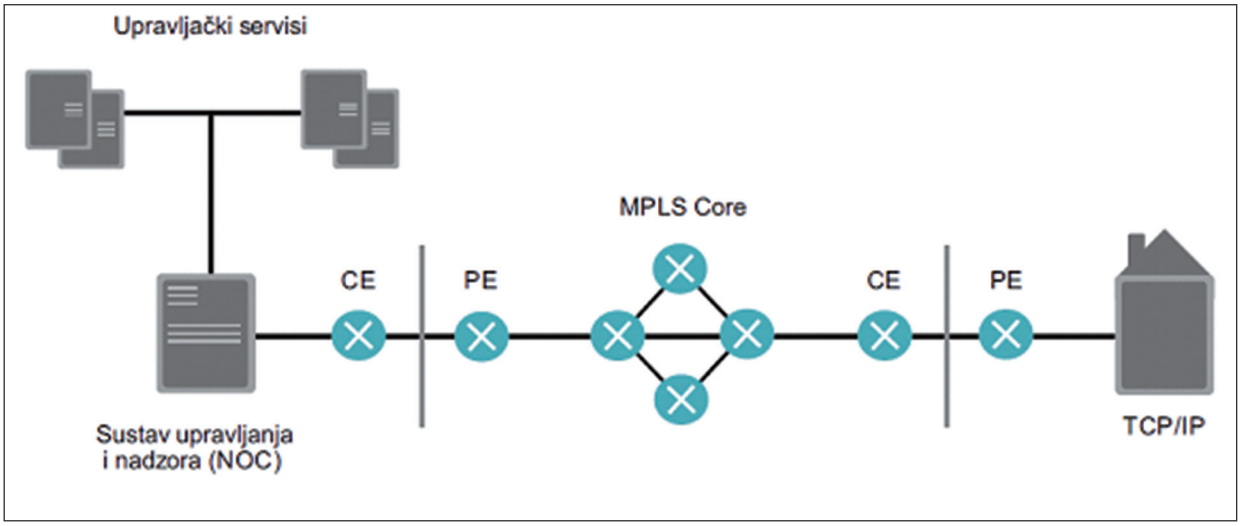

Fig. 3 *– Using Smart Grid Technology in Energy Distribution Systems*

routers, servers, and workstations. SNMP has gained widespread popularity because of its simplicity and because it is easy to implement, install, and use. Also, when used with care, SNMP does not over utilize the network. Interoperability between SNMP implementations from different vendors can be achieved with minimal effort because SNMP is simple. SNMPv3 will replace SNMP versions 1 and 2 because of security features implementation including authentication, to protect against modification of information, and secure set operations for the remote configuration of SNMP-managed devices.

Remote Monitoring (RMON)

IETF developed the RMON MIB to provide Ethernet traffic statistics and fault diagnosis. RMON agents gather statistics on cyclic redundancy check (CRC) errors, Ethernet collisions, packet-size distribution, the number of packets in and out, and the rate of broadcast packets. The RMON alarm group lets a network administrator/engineer set thresholds for network parameters and configure agents to automatically deliver alerts to NMSs. RMON also supports capturing packets (with filters if desired) and sending the captured packets to an NMS for protocol analysis. [1]

Net Flow

Collecting Net Flow data helps a network administrator/engineer to visualize traffic patterns so that proactive problem detection is possible, it also allows implementation of resource utilization (accounting). Recommendation is to carefully plan Net Flow deployment, with Net Flow services activated on strategically located routers, usually routers on the edge of a network. Although Net Flow has a performance impact on routers, the impact is minimal and is less than the impact of RMON. The benefits of Net Flow information gathering, when compared to SNMP and RMON, include the greater detail of data collected, the time stamping of data, support for different data being gathered on different interfaces, and greater scalability.

Management Information Bases (MIB)

A MIB stores information gathered by the local management agent (computing process) on a managed device. Each object in a MIB has a unique identifier and network management applications use the identifier to retrieve a value of specific object. [1]

5. Network Security

Security design is one of the most important aspects of a network implementation. Increased threats from inside and outside the network require the most up-to-date security rules and technologies. Security implementation goal should be that security problems should not disrupt the ability to provide business services, in this particular case transport of real-time data to manage smart grid network. Network design should offer a solution against attacks on real-time business data and other network elements to be damaged or accessed inappropriately.

Developing an effective security strategy and implementing this strategy to also effective security policy is a complex task. Security implementations can add to the cost of deploying and operating a real-time data transportation network. Strict security policies can also affect the productivity, especially if some ease of use must be sacrificed to protect resources and data. Security can also affect the redundancy of a network design if all traffic must pass through encryption devices, for example.

Common practice is to build systems with just enough security to bring potential losses from a security breach down to a desired level. A practical goal should be that the cost to implement security features does not exceed the cost to recover from security incidents. [5]

5.1 Identifying Network Assets

First step in security design is identifying the assets that must be protected, their value and the expected cost associated with losing these assets if a security breach occurs. Network assets include hardware, software, applications and data. Additional to that, assets also include intellectual property, trade secrets, and a company reputation (imagine security breach to NSA IT infrastructure). Some of the most important network assets are the networking devices themselves, including servers, switches and routers, and especially the firewalls and intrusion detection systems (IDS) that provide security

services to network users. These devices are attractive targets to hackers and must be hardened (strengthened) against possible attacks. [5]

5.2 Security Risks

Security risk analysis, consequent building of a security policy and secure network design is a continuous process, because of the fact that risks change in their severity on a regular basis. [3], [5]

Following security risk examples can arise if information security is breached:

- Data flowing through the network can be intercepted, analysed, altered, or deleted, compromising integrity and confidentiality;
- Related network services, which rely on trust among network devices, can be compromised, i.e., bad routing data or incorrect authentication information could be injected into the network;
- User passwords can be compromised and used for attacks other networks.
- The configuration of the device can be altered to allow connections that shouldn't be allowed or to disallow connections that should be allowed. [8]

5.3 Reconnaissance Attacks (IP scans)

Reconnaissance attack provides information about potential targets and their weaknesses and is usually carried out in preparation for a more focused attack against a particular target. Reconnaissance attackers use tools (nmap, Nessus) to discover the reachability of hosts, subnets, services, and applications. In some cases the tools are relatively sophisticated and can break through firewalls. [4]

5.4 Denial-of-Service Attacks

Denial-of-service (DoS) attacks target the service availability of a network, host, or application, making it impossible for legitimate requests to gain access to service. DoS attacks can easily interrupt business processes and are relatively simple to conduct, even by an unskilled attacker. DoS attacks include the flooding of public servers with enormous numbers of connection requests, rendering the server unresponsive to legitimate users, and flooding of network connections with random traffic, in an attempt to consume as much bandwidth as possible.

Distributed denial-of-service (DDoS) attacks are even worse than DoS attacks because the attacker targets multiple hosts, from various networks, to attack the target.

DoS attacks also take advantage of a host's or application's failure to handle unexpected conditions, such as maliciously formatted input data or a buffer overflow. DoS attacks are one of the most significant risks that a company must recognize and manage, because they have the capability to cause significant downtime. [5], [8]

6. Conclusion

With implementation of smart grid technologies, the power industry and energy service providers will undergo through the biggest change in near history. Smart grid technology will require the deployment of millions of electronic devices in a home environment, buildings and industry installations. [7]

Over the next period of time energy service provider companies will need to:

- Select end point devices – meters and sensors;
- Build a reliable communication infrastructure to connect and manage them;
- Integrate numerous head end systems (smart devices aggregation);
- Deploy data storage and management solutions to handle the vast amount of data;
- Implement sophisticated decision support systems to optimize the grid operation and deliver the smart grid benefits;
- Implement with cost efficiency, reliably and reliably [6], [7]

To success in this endeavour following points should be in tightly view of project authority:

- Implementation of comprehensive strategy that considers business, technical and regulatory requirements;
- Robust IP telecommunication system architecture with function of connecting all endpoints to the central systems (as described here in this article);
- Gaining operational knowledge with field pilot programs that is well integrated with IT and field operations;
- Organizational change strategy to address the impact this massive technological change.

Smart grid technology is here and now, energy service provider companies should adapt to this new technology scenario and implement it.

7. Reference

[1] RFC - http://www.ietf.org/rfc.html

[2] Priscilla Oppenheimer – Top-Down Network Design, Third Edition, Cisco Press

[3] Keith Hutton, Mark Schofield, Diane Teare – Designing Cisco Network Service Architectures, Second Edition, Cisco Press

[4] Andy Sholomon, Tom Kunath – Enterprise Network Testing, Cisco Press

[5] Omar Santos - End-to-End Network Security Defense-in-Depth, Cisco Press

[6] CiscoEXPO2011 – Pametne električne mreže i pametna brojila za kućanstva budućnosti

[7] CiscoEXPO2011 – Kako do energetskog certifikata; Upravljanje energijom kao mrežna usluga

[8] Article from Internet, Smart Grid & Cybersecurity – NEMA http://www.nema.org/gov/energy/smartgrid/upload/Smart_Grid_Today-04-14-09.pdf

AUTORI

Goran Kišan

Goran Kišan, ing. el. i stručni specijalist inženjer informacijskih tehnologija diplomirao je 2014 g. na specijalističkom diplomskom stručnom studiju informatike, Tehničkog veleučilišta u Zagrebu (TVZ). Tijekom preddiplomskog stručnog studija elektrotehnike u veljači 2009 g. pokreće i razvija ICT Management, servis za pružanje internetskih usluga.U svibnju 2013 g. osnivaSPARTACUS RJEŠENJA j.d.o.o. za računalne djelatnosti i usluge. Od lipnja 2013. zaposlen je u međunarodnoj prijevozničkoj i špediterskoj službi In Time d.o.o. - TNT Global Express na poziciji sistemskog inženjera gdje je zadužen za održavanje mrežne i računalne infrastrukture koja uključuje 5 poslovnica i 160+ djelatnikana Hrvatskom tržištu.

Silvi Kolarić

Silvi Kolarić, dipl. ing. el., diplomirao je Elektrotehniku 1996 g., smjer Automatizacija - Infomacijska Tehnika na Visokoj Tehničkoj Školi u Darmstadtu (Hochschule in Darmstadt, University of Applied Sciences) s naknadnim postupkom nostrifikacije diplome 1997 g. na Fakultetu elektrotehnike i računarstva (FER) u Zagrebu. Zaposlen je u firmi EagleBurgmann GmbH & Co. KG (EBG), Wolfratshausen kao inženjer mreža i računalne sigurnosti u odjelu Group IT Infrastruktura gdje je zadužen za planiranje, administraciju te vođenje projekata za lokalnu i globalnu mrežnu i računalnu infrastrukturu koncerna EagleBurgmann (Wolfratshausen, Pune, Frankfurt, Huston, Tokyo).

Zoran Baus

Prof.dr.sc.Zoran Bausrođen je 1951., diplomirao 1975.,magistrirao 1987., doktorirao 2004.god. na Fakultetu elektrotehnike i računarstva (FER) u Zagrebu. Glavno područje njegovog znanstvenog istraživanja je inteligentno upravljanje i optimizacija procesa u elektroenergetskom sustavu. Dobitnik pet međunarodnih stipendija, kao doktorsku specijalizaciju na američkom MIT-u (Massachusetts Institute of Technology). Na temelju međunarodnog natječaja za dodjelu financiranih projekata iz predpristupnih fondova Europske Unije iz Bruxelles-a, dodijeljen mu je 2004. god. projekt pod nazivom „Wireless Sensors“., iz fonda ITEA 1 (Information Technology for European Advsncement). Sljedeće godine, 2005. dodijeljen mu je novi projekt iz fonda ITEA 2, pod nazivom „4D Graphics and Animations“. Zaposlen je kao izvanredni profesor na elektrotehničkom fakultetu u Osijeku (ETFOS).

Mr. sc. Dubravko Žigman- nepromjenjena biografija nalazi se u časopisu Polytechnic & Design Vol. 2, No. 1, 2014.

Krunoslav Rukavina

Krunoslav Rukavina diplomirao je na TVZ-u u Zagrebu 2008 g. na preddiplomskom stručnom studiju informatike. Nositelj je nekoliko priznatih industrijskih certifikata CCNA, CCNP, CCDA, CCNA Security, Comptia Security+, IBM - QRadar i McAfee te također piše za IT Security časopis [Hack]in(Sight). Punih pet godina radnog staža proveo je na poziciji voditelja IT odjelaumeđunarodnoj prijevozničkoj i špediterskoj službi In Time d.o.o. - TNT Global Express.Karijeru u području informatičke sigurnosti nastavlja u firmi The Herjavec Group na poziciji Junior Security Analyst gdje je zadužen sa sigurnosna pitanja stranaka iz Kanade, Amerike i UK. Danas je zaposlen u firmi ING Management Services s.r.o. na poziciji Senior Security Analyst sa prebivalištem u Pragu.

Tihomir Car

Tihomir Car, ing. el. i stručni specijalist inženjer IT-a, diplomirao je na TVZ-u u Zagrebu 2013. Uz to stekao je certifikate iz područja mrežnih tehnologija i to CCNA, CCNP Routing & Switching te CCNA Security. Svoju karijeru započeo je u području optičkih telekomunikacijskih sistema radeći za Markoja d.o.o., nakon čega radi kao sistemski administrator u Hrvatskom Crvenom križu u Novoj Gradišci te mrežni konzultant i inženjer za tvrtku SPARTACUS RJEŠENJA j.d.o.o.s kojom surađuje i danas.