Sistemi radijskih zvez za prenos digitalnih podatkov malih kapacitet v Aktivnih omrežjih

Elior Mehr[1], Jože Štuflek[2], Aleš Blaznik[3],Tomaž Mavec[3]
[1]4RF
elior.mehr@4rf.com
[2]IT-100 d.o.o.
joze.stuflek@it-100.si
[3]Elektro Gorenjska d.d.
tomaz.mavec@elektro-gorenjska.si

Povzetek – Dokument predstavlja nove pristope k IKT tehnologijam v distribucijskih omrežjih. Predstavljene so rešitve sodobnih ozkopasovnih IP radijskih sistemov od srednjenapetostnega do prenosnega elektroenergetskega omrežja. Uporabljena je digitalna pristopovna radijska tehnologija na licenciranem ozkopasovnem VHF/UHF spektru, ki je pomembna in primerna tehnologija za SCADA komunikacije. Zadnje verzije, ki uporabljajo najmodernejše modulacijske sheme so primerne tudi za uporabo v sistemih, kjer si različne aplikacije delijo enotno komunikacijsko pot.

Radio communication systems for the transfer of digital data of small capacity in Smart Grids

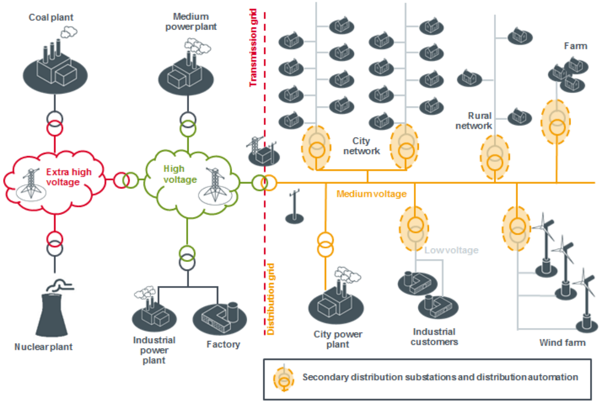
Elior Mehr[1], Jože Štuflek[2], Aleš Blaznik[3],Tomaž Mavec[3]
[1]4RF
elior.mehr@4rf.com
[2]IT-100 d.o.o.
joze.stuflek@it-100.si
[3]Elektro Gorenjska d.d.
tomaz.mavec@elektro-gorenjska.si

Abstract – This paper presents approaches to new ICT technologies seen on power distribution network. In the document solutions of modern Narrowband Licensed Wireless Communications are described. For medium voltage, at the distribution grid until the transmition grid. The technology which is been used is a digital point-to multipoint radio systems using narrowband licensed VHF/UHF wireless communications, which is an important and very relevant technology for SCADA communications. Latest versions of mentioned systems are also relevant for the use in systems where multiple applications share network resources.

I. INTRODUCTION

Digital wireless communications replaces old analogue wireless communications. The new technology challenges the new emerging markets and requires scalability to support multiple SCADA protocols and different traffic types such as RS-232 serial and IP.

Modern IP networks demand more capacity, strong security, management and flexibility.



Picture 1: Applications in the electricity grid

II. TRANSITIONING FROM LEGACY SERIAL TO IP

The world is migrating from the use of legacy serial protocols and network infrastructure through to IP-based systems.

The benefits of IP, and IP SCADA networks, are becoming clearer. However, IP also brings additional security concerns that need to be addressed.

Equally clear is the fact that this migration will not happen immediately. Vendors need to support users with equipment that is both backwards-compatible and future-proof.

The digital radios have been designed with this future-proof approach in mind; Plan for the future, protect the past. The best of both worlds

Transitioning from:

Licensed options

- VHF – long range 150 to 174 MHz with reasonably large antennas
- UHF – moderate range 400 to 470 MHz / 320 to 400 MHz and convenient antennas sizes
- 1 to 10 Watt multipoint radio, typically with directional antennas at remote sites

Radio systems

- Old analogue systems operated at speeds between 300 and 1,200 bit/s in 25 kHz channels
- Old modems use audio tones over FM radio systems
- Digital systems provide serial 9,600 bit/s and 19,200 bit/s
- **New digital systems carry RS-232 serial and IP traffic up to 120 kbit/s**

SCADA equipment is evolving to support IP. The benefits of IP mean that the latest generation of SCADA remote devices are IP based, with many advantages:

- Low cost, reliable, and scalable
- Widely accepted, a proven standard
- Network compatibility and interoperability between devices
- Multiple applications share network resources
- Bandwidth-efficient
- Use over virtually any physical medium

The benefits of an IP SCADA network:

- Over-the-air control of remote devices, e.g. SNMP
- Interoperability between devices
- Reduced infrastructure and maintenance
- Reduced requirement to visit remote sites
- Ease of interface to modern PC and server systems
- Common cabling systems

However, there is a huge deployed base of older generation SCADA systems using serial RS-232/V.24. So these legacy connections must be considered.

Regulatory pressure and cyber security concerns may mandate a security upgrade of existing serial network. Most SCADA radios today can secure both serial and IP traffic.

III. SECURITY

Licensed point-to-multipoint SCADA radios enable a comprehensive, in depth approach to security to be adopted, while providing you with flexibility, ownership and control of your network.
The solution should provide:

- Over the air protection
- Protected management interfaces
- Secure USB software upgrades

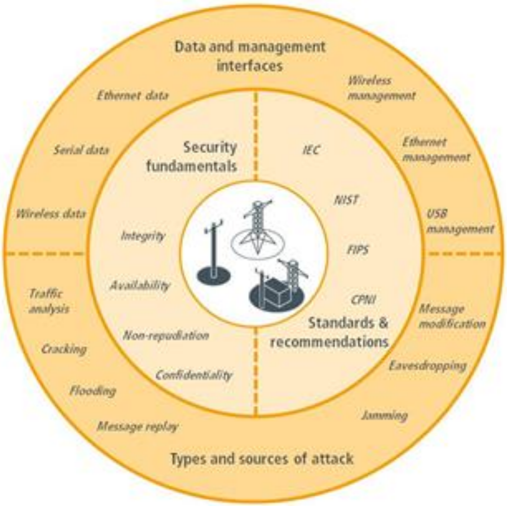
- Micro-firewalling Ethernet interface
- Using government standards and best practice

Security is more than just encryption: it needs to be designed into every part of the network to provide comprehensive, multi-faceted defence in depth. SCADA security must:

- Take into account the recommended reference designs for industrial control systems
- Build upon the best in class from multiple standards bodies, including IEC/TR 62443 (TC65) "Industrial Communications Networks – Network and System Security" and IEC/TS 62351 (TC57) "Power System Control and Associated Communications – Data and Communication Security"

This approach means securing the perimeter around the digital radio system and the design environment of the product – all external ports must be considered:

- Licensed radio spectrum
- Standardized, extensively tested wireless protocols
- Recognised encryption techniques: AES-128/256
- Authentication, including data authentication



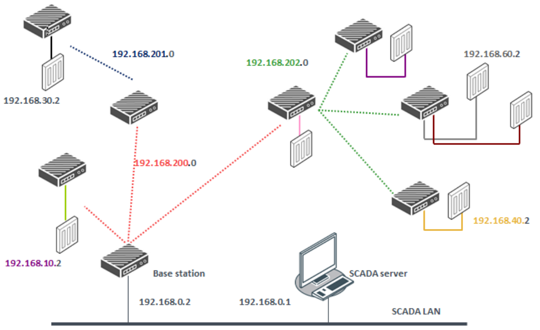
Picture 2:Security approach

Using IP, a more comprehensive approach to security can be taken:

- Address filtering
- Segregated traffic flow: VLAN, L3 subnet
- Distributed L3 firewall
- Add additional security features through Layer 3 network integration

IV. Layer 3 Network Integration

The structure is not flat, which is useful for dense networks with many branches. A message will not be broadcasted and propagate through all branches, but will be routed to the correct branch. The network capacity will be greater than in the layer 2 (flat) cases. Layer 3 network integration provides support for additional security features such as distributed firewall and address filtering. All Ethernet ports may be separate subnets, including the wireless interface



Picture 3:L3 network integration

V. Narrowband Licensed Wireless Communications

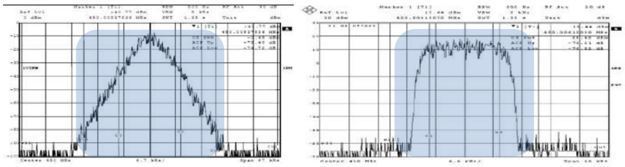
Using narrowband licensed radio remains an important and very relevant technology for SCADA communications.

- UHF/VHF frequencies are available and protected by the regulators
- Narrowband has been used for decades for mission critical communications for SCADA and public safety organizations
- Narrowband allows for greater distance and the modulation has been proven to be robust to interference
- Topologies allow for increased filtering to provide extra RF blocking protection in congested base station locations

New generation narrowband licensed radio technologies are using more efficient QAM modulation and more efficient coding options allowing them more complete use of the spectrum resource giving them many times the throughput with same system gain

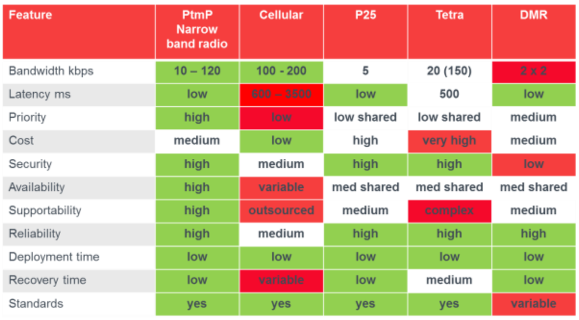
- At QPSK (lowest modulation level) doubled the capacity with the SAME range

- Even at 64 QAM (highest modulation level), the provides exceptional system gain performance and traffic up to 120 kbit/s



Picture 4:Capacity using QPSK vs.capcity using 64QAM

VI. DIFFERENT RADIO TECHNOLOGIES



Feature	PtmP Narrow band radio	Cellular	P25	Tetra	DMR
Bandwidth kbps	10 – 120	100 - 200	5	20 (150)	2 x 2
Latency ms	low	600 – 3500	low	500	low
Priority	high	low	low shared	low shared	medium
Cost	medium	low	high	very high	medium
Security	high	medium	high	high	low
Availability	high	variable	med shared	med shared	med shared
Supportability	high	outsourced	medium	complex	medium
Reliability	high	medium	high	high	high
Deployment time	low	low	low	low	low
Recovery time	low	variable	low	medium	low
Standards	yes	yes	yes	yes	variable

VII. CONCLUSIONS

Today, mission-critical SCADA networks are facing a balancing act.

Managing complexity:

- Securely monitoring and controlling a rising number of network devices
- Operating in a mixed world of serial devices and increasingly IP-based world
- Protecting the huge investment in legacy serial equipment
- While controlling the business and keeping a tight control on OPEX and CAPEX, an innovative wireless technology is required to ensure a risk-free transition to IP-based SCADA:
- Narrowband licensed radio communications is a robust and reliable technology which been used as analogue systems for few decades.
- With the new SCADA protocols been adopted, new demands for innovative narrowband licensed radio is been required.
- Smart SCADA radio – should meet the following requirements:
- Support for both serial and IP traffic in a single box
- Carry massive traffic in narrowband license radio, required a traffic compression
- Narrowband license radio required to cover long distance and the modulation scheme need to be robust against interference
    - Support multiple SCADA protocols
    - Support high capacity IP traffic
    - Security-conscious:defense in depth as part of product design
    - Easy to manage: comprehensive, but simple and secure network management
    - Standards-based: and firmware upgradeable as standards evolve to support future demands

REFERENCES

[1] 4RF

[2] IEC/TR 62443 Industrial communication networks - Network and system security - Part 3 1: Security technologies for industrial automation and control systems