SERVICE QUALITY ASSURANCE IN THE IP NETWORKS FOR SMART GRIDS

Peter CEFERIN
Smart Com – Slovenia
peter.ceferin@smart-com.si

Zvonko TOROŠ, PhD
Elektro Primorska - Slovenia
zvonko.toros@elektro-primorska.si

Rasto ĐUKIĆ, MSc
Smart Com – Slovenia
rasto.djukic@smart-com.si

Igor ŠTIH
Smart Com – Slovenia
igor.stih@smart-com.si

Brane ZUPAN
Smart Com – Slovenia
brane.zupan@smart-com.si

ABSTRACT

This paper describes innovative method of ICT network infrastructure monitoring for vital network services required in DSO's Smart Grids environment. Services monitored are of fundamental importance for connectivity and data flows between DSO's Control Centre and remote Substations and their specific Smart Grid applications. The paper deals with the concept and some Use Cases taken from realistic DSO environment pointing to effectiveness of the method used.

INTRODUCTION

Modern ICT infrastructure of the DSO's Smart Grids contains more and more devices, which require data connectivity. The number of devices is rapidly growing throughout the DSO infrastructure as many applications use IP protocol, which became technology of choice in the telecommunication networks of DSO's, as well as in the public fixed and mobile networks. From the communications point of view Smart Grid devices (e.g. AMI gateways and meters) integrate also the stack of ICT network protocols and parameters. Not only connectivity, but also assurance, measurement and monitoring of key parameters of IP communication services, independent of the ICT technology which carry IP datagrams, are required. The common situation for many DSO's is that mixed ICT technologies are used, e.g. private based IP/Ethernet services (based on L2 Ethernet, IP/MPLS or even some legacy technologies) together with public services from service providers (e.g. 2G/3G mobile networks, LTE and L2 or L3 VPN's over IP/MPLS).

Elektro Primorska as one of five distribution companies working for the DSO in Slovenia has a long tradition in deployment of Smart Grid applications, consequently the number of the devices which need ICT services is constantly increasing. Huge volume of devices already nowadays will get further increase in future as a consequence of migration of AMI system towards IP based infrastructure and usage of IPv6 protocol. As a result, the challenge of management of such number of devices and corresponding IP network services will appear. It will be of crucial importance to deliver service quality assurance for the number of the IP network parameters: beside measurement and monitoring of SLA parameters for the network connectivity (bandwidth, latency, packet loss and jitter) also network related services and resources (DHCP, DNS, authentication services, NTP – timing services, IP addresses engaged). All these parameters and services are of vital importance for the ICT network serving Smart Grids applications.

To address these challenges, the innovative concept of the service quality assurance was developed and implemented with the Network Infrastructure Monitoring (NIM) system described in the article. The concept was developed to provide tools for the network administrators for effective, cost optimized, secure and reliable management of IP infrastructure and services for the Smart Grids applications. The concept of NIM is transparent to the network infrastructure and equipment used, as it is based on the widely adapted communication protocols and network management standards. The architecture is developed around the system of the NIM hardware and software probes, which are mutually independent. NIM probes are located at the points, crucial for the IP network services. The concept provides also virtualization of the probes inside the specific IP network devices, such as Field Area Network (FAN) routers, located at the MV/LV Substations to aggregate IP services towards DSO Control Centre.

The solution delivered by NIM concept provides network operators visibility and control over crucial operational IP network parameters and services, important for Smart Grids applications data traffic, thus bringing operational benefit to network administrators, who need to provide required KPI's for the ICT network operation.

SMART GRIDS ICT NETWORKS SERVICES AND PARAMETERS MONITORING

The ICT networks in DSO organizations provide the communication services to its users, which are of operational nature i.e. SCADA, AMI, teleprotection, etc.,

of business nature i.e. corporate IT, telephony, data centres, etc., as well as to many new Smart Grid applications. All of them require information flows between two or more endpoints. Each service should comply with the user requirements with a set of parameters, which shall retain certain levels, providing performance and operation of services as expected. Furthermore, not only data flows performances and KPI's need to be measured and monitored, but also network service mechanisms and protocols responsible for ICT services operation. Cyber Security mechanisms in Smart Grids infrastructure to be integrated into ICT networks are of crucial importance to prevent potential security vulnerabilities with constant monitoring of at least basic security parameters.

Monitoring of vital network performance KPI's, services status and security parameters are important for the ICT network operators and administrators to prevent ICT infrastructure from service degradation or disruption. Active monitoring of ICT infrastructure operation and parameters is important prerequisite for Smart Grids application operation, as data transfer between Control Centres and IED's located at Substations or data transfer between Substations should retain required values.

There are numerous ICT networking devices available with already integrated functionalities for network KPI's and services measurements and monitoring capabilities, however using vendor dependent functionalities brings possible vendor lock-in threat to the DSO. The introduced Network Infrastructure Monitoring system represents vendor independent solution as it is designed as an overlay solution, transparent to the networking equipment and using standard based protocols.

THE PRINCIPLE OF NETWORK INFRASTRUCTURE MONITORING CONCEPT

NIM System denotes the solution enabling 24/7 active monitoring of the vital network infrastructure. It consists of three functional components: NIM active Probes, MqTT Broker and NIM Central SRA Server (Storage, Reporting and Administration). NIM System architecture is presented on Figure 1.

NIM Probes are placed on the vital points in the DSO's ICT network, from where critical network infrastructure is actively monitored. There is a wide variety of different types of NIM Probe functional deployments: from probes based on well-known hardware SBC's (Single Board Computer) platforms (such as Raspberry Pi or Banana Pro) to probes integrated with certain models of networking equipment (typically routers), or even deployed on any virtualization platform (MS Hyper-V, VMware ESX, OpenStack, Docker containers, …).
Records of network infrastructure monitoring performed by NIM Probes are reported to the NIM Central SRA Server where they are stored and rated against thresholds set. At this point alerting is also done in case of particular value exceeding its dedicated threshold.

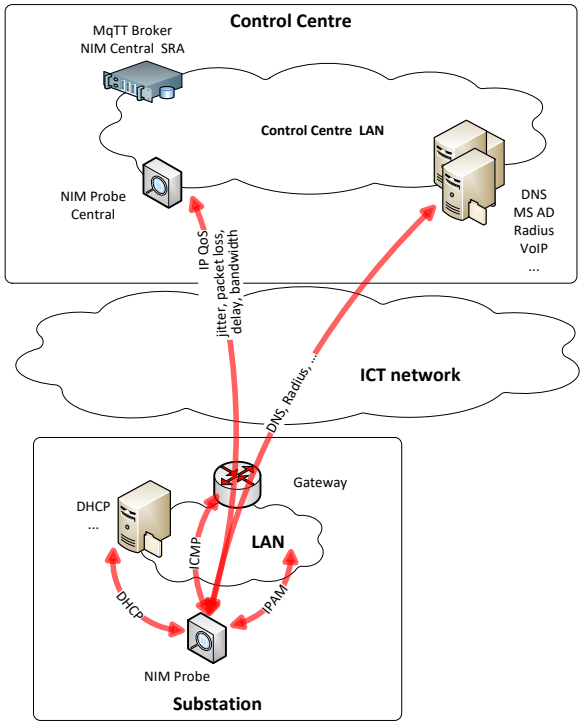

Figure 1: NIM System architecture

Beside this NIM Central SRA Server enables visualization and reporting on the network infrastructure monitoring records collected. Visualization through graphs proved to be one of the most efficient means for detecting potential KPI degradation happening on longer time span. Furthermore, NIM Central SRA Server takes care for Service Level Agreements (SLA) reports generation.

Communication between NIM Probes and NIM Central SRA Server runs via MqTT protocol. MqTT is an ISO standard (ISO/IEC PRF 20922) publish-subscribe based "lightweight" messaging protocol for use on top of the TCP/IP protocol. The publish-subscribe messaging pattern requires a message broker, in our case MqTT Broker. The purpose of MqTT Broker is distributing messages to NIM Probes or NIM Central SRA Server based on message content.

Concerning ICT network measurements performed by NIM Probes are functionally divided into three major groups: network performance KPI's, network services status and network security parameters. Generally, network performance KPI's denote set of connection-oriented KPIs that have major influence on quality of services. Network services status covers monitoring performance over a set of basic network infrastructure

support services, while network security parameters group gives an insight in DSO's network security.

Network performance KPI's

Network performance KPI's represent a set of parameters important to network operator's detailed insight into performance of data flows delivered to the users within ICT network services. Monitoring of the graphs with specific parameters and alerting operator when certain parameter value is out of required levels or thresholds is an efficient mode of operation to maintain KPI's within required SLA (Service Level Agreement) values.

Throughput is a specific measure of how much data flows over a channel (kbit, Mbit, Gbit, etc) in a given period of time (second). Throughput shouldn't be mixed with bandwidth or speed, although all three terms are related, but not identical. Bandwidth represents data capacity of a network, channel or interface, whereas speed often refers to the rated or nominal speed of a networking technology.

Latency is an IP datagram delay measured from input into a system to required output; the term is understood slightly different in various contexts and latency issues also vary from one system to another. However, latency, when transferring data in DSO ICT networks greatly affects the performance of certain applications. For example, Substation GOOSE based applications require low-latency communications with latency budgets in order of milliseconds.

Jitter in IP networks is the variation in the latency on a packet flow between two systems, when some packets take longer to travel from one system to another. Jitter results from network congestion, timing drift and route changes. Some real time applications, like IP telephony, video surveillance or teleprotection applications require low jitter values in order of milliseconds.

Packet Loss is the failure of one or more transmitted packets to arrive at their destination. This event can cause noticeable effects in all types of digital communications. Mission critical applications in DSO ICT networks require very low packet loss values.

MTU (Maximum Transmission Unit) is the size of the largest IP data unit that can be communicated in a single network transaction. Although monitoring of MTU during normal and stable operation of the services is usually not needed, this measurement is important in case of malfunctioning of the services during the phase of provisioning as MTU size of certain technologies or equipment cannot match MTU required by an application. MTU monitoring is important also in case of changes in the system either on network side, or on the application side.

TCP retransmissions - TCP/IP protocol has built-in logic for ensuring that packets are received. To ensure that, the sender will retransmit the packet to the other party if the packet is lost. However, the TCP retransmission will cause increase in latency. In such cases observing only the latency will not point to the subject of latency increase. The TCP packet retransmission value increase correlates to the latency increase. Furthermore, if there is also packet loss exceeding the threshold, this might point to the ICT network equipment failures or errors in the transmission media (Wireless, PLC, etc.).

Network services status

This group of measurements refers to monitoring of basic network infrastructure. One has to be aware that any service running over ICT network in question highly depends on those functionalities.

DNS (Domain Name System) represents the system that translates more readily memorized domain names to the numerical IP addresses needed for the purpose of locating and identifying services and devices with the underlying network protocols. By doing this DNS simplifies ICT network operational work and enables higher reliability Utility process systems.

RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users and devices who / which connect and use a network service. In the situation with ICT network becoming more and more diverse and complex it is of crucial importance to authenticate and authorize any user or end system connecting to network according to its role and importance. ICT network security therefore strongly depends on RADIUS.

NTP (Network Time Protocol) is a network protocol for clock synchronization between network devices over packet-switched, variable-latency data networks such as ICT network. It is of absolute importance for ICT network operation to have all systems and devices synchronized. If this is not the case particular network event might carry different time stamps as we stroll through the network. This impacts highly effectiveness of any troubleshooting on one hand and process systems' operation on the other.

DHCP (Dynamic Host Configuration Protocol) server enables devices to request IP addresses and network parameters automatically, reducing the need for a network administrator or a user to configure these settings manually and thus limiting possibility of misconfiguration which may in worst scenario lead to network segment, device or service discontinuation.

Network security parameters

Dedicated to network security the group of measurements described below relates to measurements needed in modern DSO's ICT networks and end devices in order to assure network operation according to newest network security standards and prevent its vulnerability.

IP address scan as a periodical measurement identifies potential IP addresses configured, but not used and by this ensures availability of network resources. In the situation of more and more limited IPv4 addresses importance of this functionality increases. The very same measurement can detect rogue IP addresses in the ICT network, pointing to potential malware situation.

For any end system application or network entity that needs to communicate over ICT network there must be approved list of ports used for that purpose. The aim of TCP/UDP port scan of ICT network is to ensure that there are no other ports open. This not being the case, one can conclude about security risk presence.

Internet ping represents rather basic but very efficient way of identifying potential unwanted network openness towards internet or some other autonomous system. The later can be used in different DSO's network segments keeping in mind crucial delineation between DSO's IT and OT domains.

IMPLEMENTATION OF NIM IN DIFFERENT ICT NETWORK SCENARIOS

Considering NIM System's flexibility and consequently wide applicability various network situations can be addressed. However, this chapter highlights three use cases selected from numerous typical situations for DSO's network.

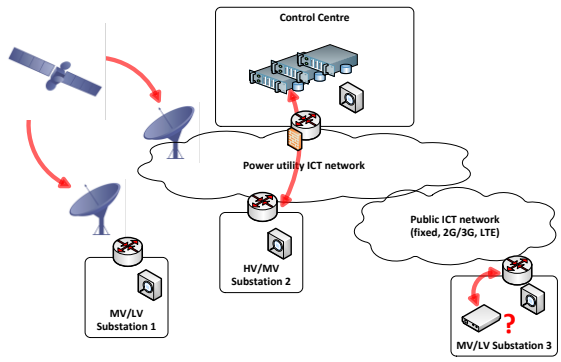

Figure 2: DSO's NW general topology

Figure 2 represents general topology of DSO's network consisting of: Control Centre location (CCL) and HV/MV or MV/LV Substation locations (SL). Control Centre location hosts SCADA System and usually various communication equipment, such as routers, firewalls, VPN concentrators and in our case also Central NIM Probe.

Communication between given MV/LV Substation location and Central location can run over different types of technology (e.g. satellite link, public or private mobile network or fixed line being optical or copper), depending on infrastructure available.

Use Case 1: Substation connectivity

At given point in time operational staff faces partial lack of control over SL1. SL 1 presented on Figure 2 is located in geographically demanding environment allowing only satellite link as a means of connection to CCL. Initial analysis shows increased packet loss on connecting link (Figure 3).

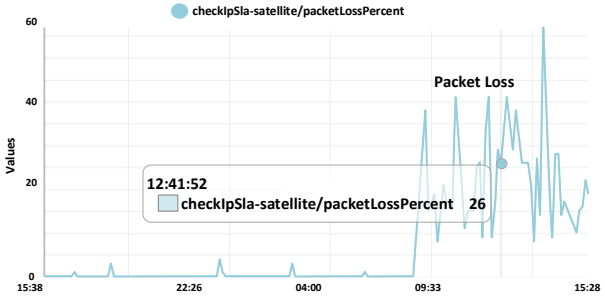

Figure 3: Packet loss measurements on satellite link

Further analysis reveals substantial bandwidth drop of SCADA traffic combined with increased number of TCP retransmissions as presented on Figure 4. TCP retransmission increase (dark green line) becomes less evident with both graphs using same scale.

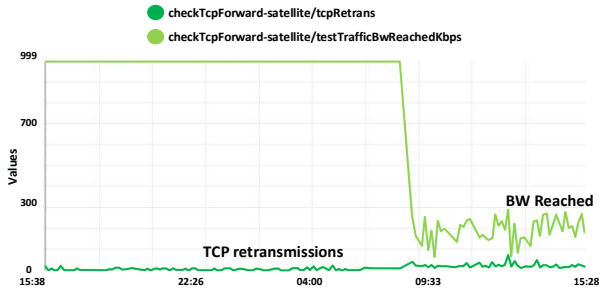

Figure 4: Bandwidth (light green) and TCP retransmission (dark green) measurement on satellite link

Firstly, Substation communication gateway is suspected, but after deeper investigation in what could be the reason for bandwidth degradation it is found that monthly amount

of rented traffic was consumed and as a consequence traffic was rate-limited by satellite operator. As a counter measures agreement with satellite operator about increasing monthly amount of traffic and SCADA traffic prioritization on communication gateway takes place.

Use Case 2: Substation unreachability

Suddenly, DSO's network starts to show strange behaviour. Some SLs and systems cannot be reached while others seem to be accessible. All services are degraded, but to different extent. Verification of all systems on Control Centre location points to ICT network problem. Starting on demand ping test on IP addresses for some SLs proves successful indicating there is no problem with connectivity. Further analysis of basic network services shows DNS service outage as presented on Figure 5.

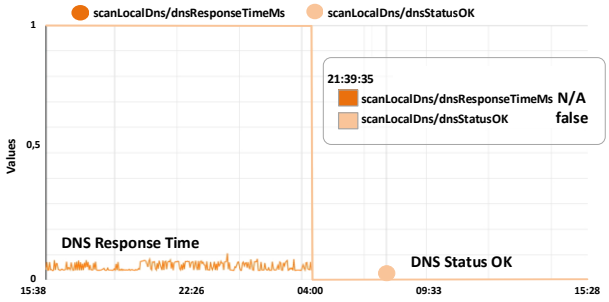

Figure 5: DNS availability measurement

As a short-term solution DNS service on DNS Server is restarted. As a long-term and more reliable solution redundant DNS Service is introduced.

Use Case 3: Unauthorized device

Beside monitoring all network services and network performance KPI's ICT operational staff has to have an insight on what devices are being connected on any given location. This is one of the prerequisites for maintaining DSO's network secure.
On SL3 as presented on Figure 2 normally there are five IP addresses active including router interface. Unexpectedly sixth IP address is detected, represented by question mark. Figure 6 represents IP address increase for location in question.

This information is available thanks to regular IPAM (IP Address Monitoring) scan as set on NIM Probe. For the scan in question alerting in case of such event is set. As presence of unwanted IP address indicates unauthorized access and consequently security policy violation, this IP address is blocked remotely and field technician sent to location.

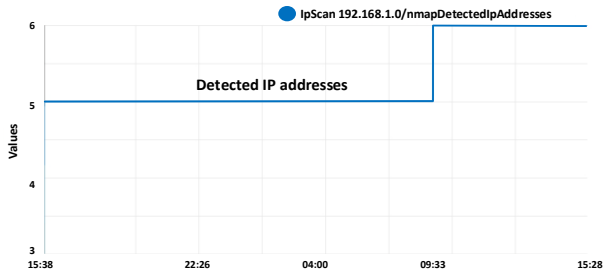

Figure 6: IPAM measurement

CONCLUSIONS

ICT networks have important role in operation of modern DSO Smart Grids infrastructure as connectivity and data transfer between Control Centre and Substation IED's and between IED's is fundamental for DSO power network operation and control. Nowadays many communication network technologies in operation bring required services, being in private or public networks. To achieve ICT network services control and visibility measurements and monitoring of network performance KPI's, network services status and network security parameters is necessary. In the article presented concept of Network Infrastructure Monitoring system provides ICT network operators from DSO like Elektro Primorska efficient toolset to perform network services quality assurance. Described use cases show few selected situations from real ICT network operation, where NIM system proved its efficiency. Many additional parameters or network services can be added into the system, further work on the NIM will be focused on additional security monitoring functionalities, as cyber security mechanisms are introduced into ICT networks to prevent potential cyber-attacks and vulnerabilities. Further work will be also to extend the integration of probes into virtualised environment, especially with the FAN routers, as communication node at the MV/LV Substation level.

REFERENCES

[1] P.Ceferin, Z. Toroš, R. Đukić, I. Štih, A. van Wonderen, B. Zupan, 2015, "Management of SLA parameters in ICT networks for Smart Grids", *CIRED 2015, Lyon*

[2] P.Ceferin, Z. Toroš, R. Grobin, I. Štih, J. Cukjati, 2013, "Methodology of throughput tests in telecommunication networks for MV/LV substations", *CIRED 2013, Stockholm*