Journal of Engineering and Applied Sciences 14 (Special Issue 5): 9036-9041, 2019
ISSN: 1816-949X

High Availability in Hybrid Network Smart Grid Environment

Ladislav Balik, Ondrej Hornig and Vladimir Sobeslav
Department of Information Technologies, Faculty of Informatics and Management,
University of Hradec Kralove, Hradec Kralove, Czech Republic

Abstract: This study presents a solution for achieving highly available network in smart grid environment with hybrid network infrastructure in a form of a case study. It presents an approach of using custom mechanisms in cases when there cannot be used any standard solutions. This study describes several standard mechanisms, such as HSRP synchronization and IPsec stateless failover. Furthermore, these mechanisms are completed with routing optimization and event triggering based on custom status and event monitoring.

Key words: High availability, smart grid, networking, electrical grid, HSRP synchronization, IPsec

INTRODUCTION

Smart grid is a concept used to include the application of secure, two-way communications and information technology to electrical power grids (IEEE). This approach enables to flexibly react to shifts in energy consumption, adjust energy production and real time grid monitoring. It is very complicated to store large amounts of energy (e.g., use of pumped hydroelectric storage) therefore, contributions of smart grid are inconsiderable and deployment of smart grid is a ubiquitous trend in power grids.

The usual smart grid architecture uses a central point (or points) for monitoring and control. This study focuses mainly on data networks used for communication between central point, substations and separate reclosers. Although, island operation is generally possible, this approach is critically dependent on real-time communication with individual substations and other elements in smart grid. Such communication technology represents critical infrastructure which smart grid is naturally a part of. Communication infrastructure has to be opened up appropriately. Components, communication lines and used protocols must be chosen carefully. Interoperation of these components allows achievement of highly available network which is robust enough to be highly resilient. High availability provides necessary reliability when even in case of failure of key component, the infrastructure is still able to provide services for communication in the same or at least sufficient quality. In combination with high availability is necessary to provide an appropriate security based on legislative requirements (Wang and Lu, 2013). This goal is achieved mainly by securing physical access, encrypting data communication channels and using access control framework with secure central authentication, Authorization and Accounting of All users (AAA). The need of both high grade security and reliability presents a challenge for used approach in design of network architecture, choice of protocols and overall system tuning. Hybrid computer network environment is a computer network which is used not only for smart grid operation but as a general industry data network that uses technologies mainly avoided in smart grid oriented networks. This hybrid environment presents a further challenge for achieving above mentioned goals.

This study presents a solution of redundantly interconnected IPsec concentrators in hybrid environment of existing industry network of one major energy distributor in Czech Republic. This solution is presented in a form of a case study and is currently deployed.

MATERIALS AND METHODS

State of the art: Data network in smart grid acts as a support network for an energy grid transferring electricity. Grid control and monitoring has to be possible from multiple locations: from consumer endpoint from individual substations and also from central control room. Voltage spikes and fluctuations has to be eliminated same as current passage has to be routed through lines with sufficient capacity or through backup lines (e.g., for malfunction or maintenance).

Inner architecture of substation network is derived from IEC 61850 standard. Horizontal communication presents a main network used for IED (Intelligent Electronic Device), specifically for GOOSE and GSSE communication, commanding, state and event gathering

Corresponding Author: Ladislav Balik, Department of Information Technologies, Faculty of Informatics and Management, University of Hradec Kralove, Hradec Kralove, Czech Republic

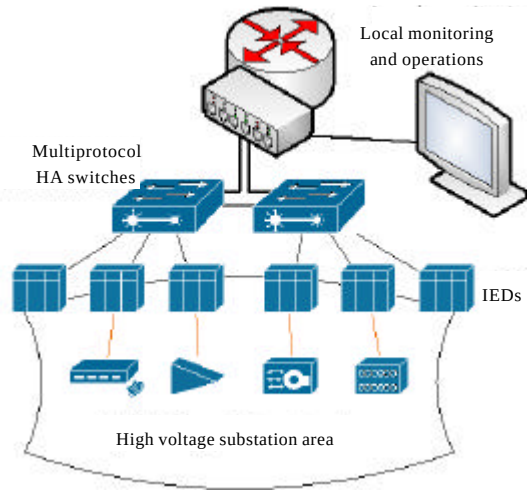

Fig. 1: Substation schema with remote connection router and SCADA terminal

in distribution network (Hoyos *et al*., 2012). These messages are encapsulated into ISO 802.3 Ethernet frames with various modifications where IEC 61850 adds a mechanism for reliable and fast delivery on ISO/OSI data-link layer (Kriger *et al*., 2013).

Security: Two main areas of security are crucial for boths substations and control. These are communication security and access security.

Communication security as an end-to-end security is a term widely used in smart grid theory and requirements. Multiple solutions are available but only the highest security standards are suitable for such a highly critical infrastructure. FIPS (Federal Information Processing Standards) and guidelines acts as an appropriate framework to be used in smart grid but it is important to appreciate its limitations and take them more as a mandatory minimum, than a level of security to achieve (Holik *et al*., 2015). For example, it is possible to use encryption algorithms in Czech non-government sector which would be limited by law in America and available only for government projects.

Originally IEC 61850 GSE (GOOSE and GSSE) messages was meant to be confined within substation horizontal network that is shown on Fig. 1. Now a days their use is often extended to WAN networks (Hoyos *et al*., 2012). Although, IEC 62351 brought some security mechanisms to GSE, use of secure tunnelling mechanisms ensures generally higher level of security.

In a perspective of securing communication between substations and among WAN lines, the use of gateway-to-gateway security architecture presents ideal solution. This approach is reasoned also by fact that often inter-substation communication infrastructure supplier is different from the one supplying SCADA (system for remote monitoring and control). SSL/TLS protocol is becoming more and more popular for use in VPN solutions but although its wide spread brings further improvements to its security and functions, IPsec still presents much more secure solution overall. Its main advantage is its framework architecture that enables use of different algorithms for and much wider possibilities in term of additional adjustments to specific needs of local environment (Cisco Systems, 2008). IPsec allows to use SHA512 hash algorithm and 256 bit AES encryption.

As in every branch of businesses also in energy industry, there is a significant growth in need for remote access and also its security. Distinct suppliers need to access delivered and supported technologies. Different VPN solutions are deployed on border firewall of technological data network. Central AAA server usually connected to LDAP or AD DS is used to verify users and distribute access rules to devices in smart grid network. Less smart but also usable approach is to deploy ACLs on every device or central firewall.

Reliability: Reliability is inherent for any critical infrastructure. Architecture that is operated in 24×7 regime and ensures unaltered operation even in case of malfunction is called highly available. High availability in term of data network consists mainly of three parts:

- Redundant hardware components of network devices
- Inter network device redundancy
- Network lines (paths) redundancy

Redundant components used in networking devices provide higher reliability and enables network devices to withstand a single component malfunction. Mutual cooperation of devices which are able to backup each other's role, brings redundancy to a higher level to redundant devices (Graham, 2015).

Use of redundant devices directly require to use a redundant network line topology (multiple lines from communication source to destination). Combination of these mechanisms allows to achieve a fully redundant topology where failure of one component, being either device, its component or a communication line does not significantly affect performance of the whole network.

Uninterrupted operation of the whole high available network is supported by the use of different network protocols such as First Hop Redundancy Protocols (FHRP), dynamic routing protocols and protocol failover mechanisms (e.g., IPsec failover) (Kocharians *et al*., 2014).

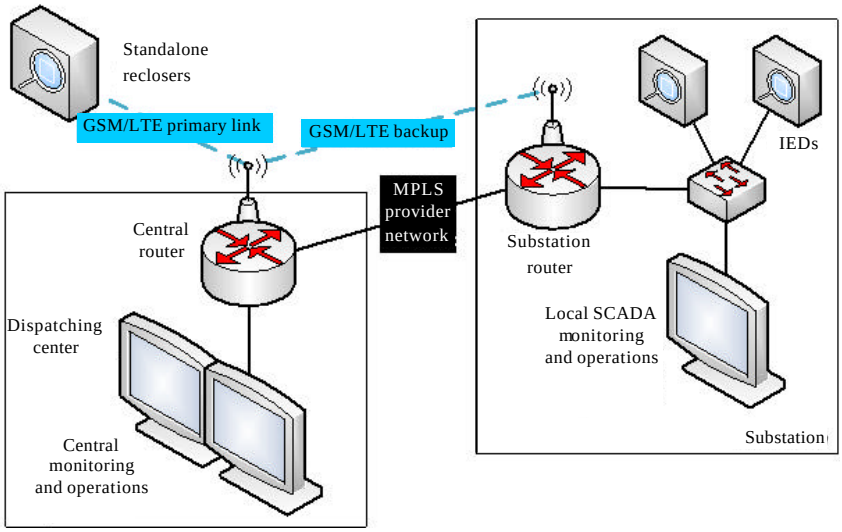

Fig. 2: Smart grid network for monitoring and operations schema

Specifics of local environment: Main part of presented network topology consists of individual substations, central monitoring and operations, standalone reclosers and primary and backup network lines interconnecting individual stations and devices.

Substations are equipped with often complex set of IED's with minor SCADA system for local monitoring and operations used mainly as backup solution. Central monitoring and operations are located along one of the substations, sharing its LAN network. Standalone reclosers are used as offsite solution where there is no need for a standard substation. These reclosers does not utilize primary MPLS lines but only wireless technology used for backup communication. Figure 2 represents topology and interconnection of the above mentioned system.

Inter-substation communication: Standard IP WAN communication technologies are used for remote monitoring and commanding. Both primary and backup lines are using IPsec tunnelling. Described topology consists of around 20 substations that are interconnected with central monitoring and operations. Tunnelling uses hub-and-spoke like topology where every substation is able to securely communicate with central site. IPsec tunnelling also provides some level of control system network isolation from underlay networks.

Primary communication is provided by MPLS telco network, backup communication is ensured by private APN provided by GSM/LTE cellular network.

Network topology limitations: MPLS primary WAN network serves as a general enterprise technological network, referred as hybrid topology. Absence of topology alterability and use of technologies not always suitable for smart grid presents a major limitation. High available solution must therefore comply with technologies such as NAT which greatly limits deployability of standard solutions.

NAT limitations: MPLS network uses 172.16/.X.0/24 prefix for individual sites. Both substations and central site LAN networks uses 192.168.Y.0/24 subnets. Overlapping LAN subnets in combination with IPsec tunnelling are resolvable issue in standard networks but NAT used in the topology prevents it. As an established convention, substation smart grid systems are accessed using statically NATed WAN addresses.

Routing limitations: Described topology utilizes only static routing. Statically routed segments are unable to flexibly react to topology changes primary communication outage in this case. Remote router reachability monitoring over specified communication line (referred as IP SLA monitoring) is used for primary/backup line switchover. This is accomplished in combination with static route tracking and use of static floating routes in router configuration.

Synoptic topology with well-designed addressing plan along with suitable dynamic routing protocol provides itself a basic level of redundancy. Routing protocols often presents a security risk but in combination with update authentication and IPsec tunnelling its features overcome its risks. Unfortunately, both MPLS and cellular network providers does not allow any cooperation on dynamic routing protocol level.

Furthermore, use of NAT in the topology limits the possibilities of building OSPF topology over IPsec and GRE or IPsec and VTI.

RESULTS AND DISCUSSION

Solution proposal prototyping: Objective of the study was to propose a solution with sufficient level of high availability which enables to maintain uninterrupted communication in case of failure of any system component. Acceptable outage in case of failure has been set to a maximum of 60 sec. Control system is unable to notice such a short outage in most cases. Additional requirement was to use existing devices and preserve device unity across the whole topology.

Considering above mentioned topology limitations, using any of standard high availability solutions based on best practices is not possible. Several solution iterations were presented addressing stateful switchover, standard FHRP usage, IPsec failover, primary/backup line switching and primary/backup device switching.

Stateful switchover: It is possible to ensure uninterrupted VPN connection handover in highly available device cluster. For this case it is necessary to synchronize protocol keys. Standardized mechanism for IKE crypto keys is described in IETF RFC 6311 (Singh *et al*., 2011).

Many vendors have their own solution for this purpose implemented. Firewall devices are usually equipped with much more sophisticated synchronization technology than routers. Cisco implements IKE load balancer cooperating with first-hop redundancy protocol HSRP. It is designed for basic router series where it supports the role of VPN concentrator. RFC 5685 is implemented for redirecting IKE protocol requests (Devarapalli and Weniger, 2009). In router VPN concentrator cluster requests are redirected to the gateway that has the lowest load, so, it supports backup and load distribution in one time. IKE load balancer, same as the DHCP server is supported by Stateful Switch Over (SSO) and NonStop Forwarding (NSF) technologies (Cisco Systems, 2008).

Despite of well documented functions of SSO and NSF, during lab testing phase, this feature was found unstable and buggy even with newest IOS 15 Version. Major errors in synchronization states and total device instability occurred unexpectedly.

Approach using stateless solution with a development of custom device synchronization mechanisms with support of FHRP and IPsec tunnel reestablishment was chosen instead.

FHRP protocol synchronization and interoperation: In non-standard topologies where local-area default gateway is highly available because of FHRP protocol, WAN side high availability is usually ensured by dynamic routing protocols such as OSPF. If it is not possible to use dynamic routing protocol (for example in operating topology with static routing implemented), a need to implement second FHRP protocol on the WAN side may occur. This approach embrace a need for FHRP process state synchronization (Kocharians *et al*., 2014).

By FHRP protocol priority parameter an administrator or automatized script can control master-slave priority distribution. HSRP ability to control priority based on IP SLA tracking makes this protocol more suitable over other first-hop redundancy protocols. More IP SLA tracks can be combined together to create a complex set of rules for HSRP role switching.

IPsec failover: IPsec failover mechanisms based on RFC are widely deployed and well tested. Dead peer detection mechanism (Huang *et al*., 2004) with protocol high availability support based on IKEv2 synchronization (Singh *et al*., 2011) represents such a mechanisms. Notwithstanding these mechanisms, stateless IPsec failover had to be implemented mainly due to limitations associated with the use of NAT, described earlier.

Inability to synchronize security associations among peers presents a problem for tunnel recovery. If an active peer fails, the secondary becomes active as described above. Although, responding on the same IP address, newly active peer does not have any security association with remote substation router. Standard IPsec operation would require for remote router to wait for security association presented to timeout by SA lifetime or by dead peer detection mechanism. Ability to recover from the state when new peer receives an IPsec packet and has no SA for SPI received in packet header is needed for faster communication recovery (Basu *et al*., 2014). Mechanism allowing to create new SA based on invalid SPI reception called invalid SPI recovery address this issue.

Ipsec session creation can be (in communication point of view) a time consuming process, especially on slower or unstable lines. To further speed up IPsec session recreation, custom mechanisms allowing to pre-dial IPsec tunnel were implemented. These are based on loopback addresses, allowed to enter a tunnel, sending traffic prior to peer switchover thus, reducing time for relevant communication establish a session. This mechanism allows to reduce recovery time to less than a half needed with only dead peer detection implemented.

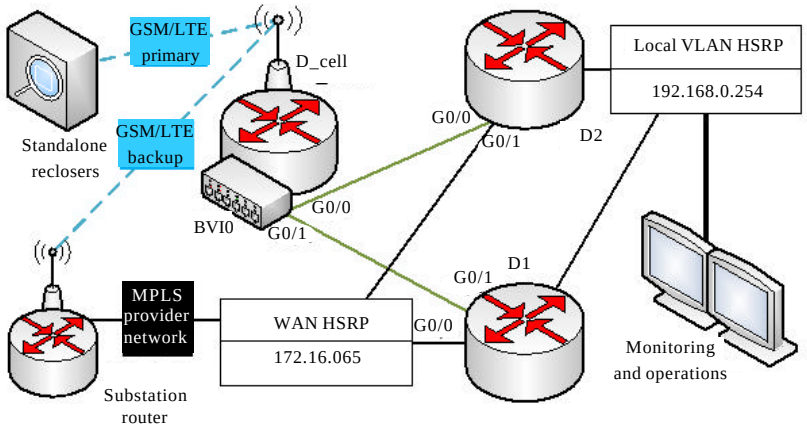

Fig. 3: High available monitoring and operations schema

Primary/backup line and device switching: As described earlier, every substation router has primary line (connected via provider's MPLS network) and backup line operated by cellular network provider. If the main connectivity between central router and substation fails, secondary wireless connection is used. Switchover is based on IP SLA information using TCP and ICMP echo messages. Well-tuned timers for monitoring and line switching are very important for line flapping avoidance and overall network stability.

Second router D2 is added to the solution to work as HSRP slave. D•CELL router takes over the cellular connection from D1. This was done because of problems with static routing combined with HSRP and mainly because of disability of standalone reclosers to participate in routing. D1, D•CELL and D2 share one L2 segment using bridged virtual interface. As shown in Fig. 3 LAN and WAN HSRP processes were implemented with combined IP SLA track ensured synchronization.

Testing and fine tuning: Proposed solution was implemented in and stress tests were performed for precise timer setup. These timers are critical for path routing between central monitoring and operations point and substations. Following combinations of single or multiple failures in central LAN, central routers or WAN connectivity were tested; Line failure in MPLS network: this will cause routing change (floating route becomes active) and all of the traffic will be delivered by backup network. Line failure in cellular network: all the standalone reclosers are disconnected (no HA required or possible), standard substations are not affected. Line failure between central monitoring station and LAN port on D1 router: HSRP primary master priority decreases, preemption takes place and D2 router becomes active. Both LAN HSRP and WAN HSRP process priorities are affected. IPsec tunnels are redialled on D2 towards all substations. Line failure between D1 and WAN providers router: same scenario as number 3. Multiple failure case: D1 WAN line failure along with D2 LAN line failure. In this case both router HSRP priorities are affected causing the traffic to be routed asymmetrically. Communication full recovery takes up to 40 sec.

After delay and timer optimization, recovery times were further reduced. In single failure scenarios, all communication recovery times are limited to the maximum of 10 sec. Scenarios where master router stays active usually takes up to 4 sec.

CONCLUSION

This study presented high availability problematics with a focus on smart grid environment and non-traditional network topology. Proposed high availability design addresses multiple specifics of hybrid network environment and presents a possible mechanisms for custom solution design and possibly the new approach for high availability implementation.

This type of solution does not intend to substitute commonly used high availability solutions but rather presents an alternative suitable for smaller smart grid implementations where deployment of dedicated smart grid network topology unacceptably prolongs a return of investment. Proposed solution circumvents different drawbacks of hybrid network without compromising security demands of smart grid.

SUGGESTION

Project testing phase revealed, that network operation recovery is generally faster and central monitoring SCADA software system is unable to

recognize network state changes. Additional incorporation in SCADA system for network state monitoring is a subject of future works.

ACKNOWLEDGEMENTS

This research and the contribution were also supported by project "Smart Solutions for Ubiquitous Computing Environments" FIM, University of Hradec Kralove, Czech Republic (under ID: UHK-FIM-SP-2016-2102).

REFERENCES

Basu, A., A.M. Chacko and W. Zhang, 2014. IPsec %RECVD_PKT_INV_SPI errors and invalid SPI recovery feature information. Cisco Systems Networking Hardware Company, San Jose, California. http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/115801-technote-iosvpn-00.html.

Cisco Systems, 2008. Cisco IOS classic firewall stateful failover high availability solution. Cisco Systems, San Jose, USA. http://www.cisco.com/c/en/us/products/collateral/routers/3800-series-integrated-services-routers-isr/white_paper_c11_472858.pdf.

Cisco Systems, 2012. VPN Availability configuration guide. Cisco Systems, San Jose, USA. http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpn-availability-15-mt-book.pdf.

Devarapalli, V. and K. Weniger, 2009. Redirect mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2). Network Working Group. https://www.rfc-editor.org/rfc/pdfrfc/rfc5685.txt.pdf.

Graham, M., 2015. Applying high availability design and Parallel Redundancy Protocol (PRP) in safety critical wide area networks. J. Telecommun. Syst. Manage., 4: 1-7.

Holik, F., J. Horalek, S. Neradova, S. Zitta and M. Novak, 2015. Methods of deploying security standards in a business environment. Proceedings of the 25th International Conference on Radioelektronika (RADIOELEKTRONIKA), April 21-22, 2015, IEEE, Czech Republic, ISBN:978-1-4799-8117-5, pp: 411-414.

Hoyos, J., M. Dehus and T.X. Brown, 2012. Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure. Proceedings of the 2012 IEEE Workshops on Globecom (GC Wkshps), December 3-7, 2012, IEEE, Colorado, USA., ISBN:978-1-4673-4942-0, pp: 1508-1513.

Huang, G., D. Rochefort and S. Beaulieu, 2004. A traffic-based method of detecting dead Internet Key Exchange (IKE) peers. RFC, Mexico.

Kocharians, N., P. Paluch and W. Odom, 2014. CCIE Routing and Switching V5.0 Official Cert Guide. 5th Edn., Pearson Education, Upper Saddle River, New Jersey, ISBN:978-1-58714-492-9, Pages: 1400.

Kriger, C., S. Behardien and M.J.C. Retonda, 2013. A detailed analysis of the GOOSE message structure in an IEC 61850 standard-based substation automation system. Intl. J. Comput. Commun. Control, 8: 708-721.

Singh, R.E., G. Kalyani, Y. Nir, Y. Sheffer and D. Zhang, 2011. Protocol support for high availability of IKEv2/IPsec. Internet Engineering Task Force (IETF). http://www.ietf.org/rfc/rfc6311.txt.

Wang, W. and Z. Lu, 2013. Cyber security in the smart grid: Survey and challenges. Comput. Networks, 57: 1344-1371.