Contemporary Trends for Increasing the Reliability of the SCADA systems Communication Level

Emiliya Dimitrova[1] and Vasil Dimitrov[2]

Abstract – **In this paper the benefits of the implementation of the open transport networks in the communication level of SCADA systems are given. OTN ensures absolute reliability. Its main features are simplicity, openness, easy integration, ability to cover very large distances, as well as the future-proof design.**

Keywords – **SCADA (Supervisory Control and Data Acquisition systems), Optical Open Transport Network (OTN).**

I. INTRODUCTION

SCADA systems are highly distributed systems used to control of geographically dispersed objects, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation. They are used in distribution systems such as electrical power grids (production and distribution of electricity), railway transportation systems, water distribution systems, oil and natural gas pipelines, etc. The purpose of SCADA systems is centralized data acquisition, information processing and visualization and generation of managerial impacts. The centralized monitoring and control of many non-concentrated subobjects (including monitoring alarms and processing status data) is performing in the Central Dispatcher Post (CDP) by long-distance communications networks. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. They control local operations such as opening and closing breakers and valves, collecting data from sensor systems, and monitoring the local environment for alarm conditions. The correct and reliable functioning of SCADA system is crucial for the functioning of the whole system [1].

II. STRUCTURE OF THE SCADA SYSTEMS

Each SCADA system is built on three formal levels [1, 2]: Upper (Dispatching) level, Communication level and Lower (Object or Field) level (Fig. 1). It consists of both hardware and software. Typical hardware includes following elements:

- Master terminal unit (MTU) – server placed at the CDP. In addition to the servers, this level includes video-walls, Dispatchers working places, personal computers, printers and the data historian, which are all connected by a LAN.
- Communications equipment (e.g., radio, telephone line, cable, or satellite) and access monitoring and surveillance systems (video cameras, sensors, and various types of identification systems).
- Geographically distributed field sites consisting of Remote terminal units (most often Programmable Logic Controllers - PLCs), sensors for measurement, actuators (i.e. breakers, switches, control valves, and motors) and Intelligent Electronic Devices (IED) – i.e. multifunction protection relays. PLC monitors sensors and controls actuators through appropriate algorithms.

The IEDs are “smart” sensors/actuators containing the intelligence required to acquire data, communicate to other devices, and perform local processing and control. Many IEDs combine analog input sensors, digital (relay) inputs, analog and digital outputs, low-level control capabilities, a communication system, and program memory in one device. The use of IEDs in SCADA systems allows for automatic control at the local level (IED act without direct instructions from the CDP). The local PLCs poll the IEDs to collect the data and pass it to the SCADA Server.

The communications hardware allows the transfer of information and data back and forth between the MTU and PLCs. The MTU stores and processes the information from objects, displays information to the monitors and video-walls, and may generate actions based upon detected events. The server is also responsible for centralized alarming, trend analyses, and reporting.

The software is programmed to tell the system what and when to monitor, what parameter ranges are acceptable, and what response to initiate when parameters change outside acceptable values.

The communication level consists of Ethernet network in the CDP, transmission medium between the CDP and object and Ethernet network in any object.

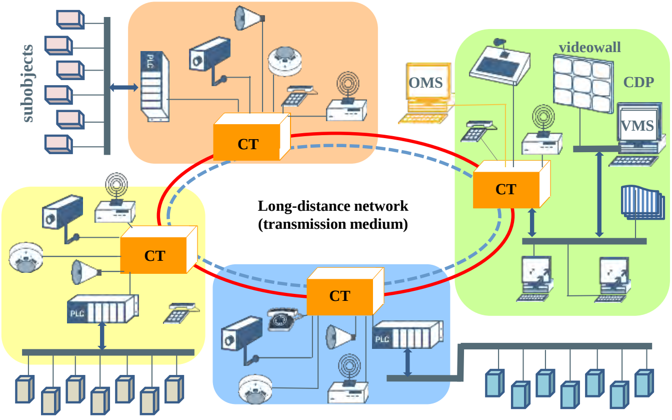


Fig. 1. Example of a SCADA system

[1] Dr. Emiliya Dimitrova is with the Faculty of Communications and Electrical Equipment in Transport at Todor Kableshkov University of Transport, 158 Geo Milev Str., Sofia, Bulgaria.

[2] Assoc. Prof. Dr. Vasil Dimitrov is with the Faculty of Communications and Electrical Equipment in Transport at Todor Kableshkov University of Transport, E-mail: vdimitroff@abv.bg

There are different network characteristics for each layer within the system hierarchy. The fieldbus network links sensors and other devices to a PLC. Use of fieldbus technologies eliminates the need for point-to-point wiring between the controller and each device. The devices communicate with the fieldbus controller using a variety of protocols. The messages sent between the sensors and the controller uniquely identify each of the sensors. The control network connects the supervisory control level to lower-level control modules. The communications terminals (CT in Fig. 1) transfer messages between two networks. Common uses for CTs include connecting MTUs and RTUs to a long-distance network medium for SCADA communication. A firewall protects devices on a network by monitoring and controlling communication packets using predefined filtering policies. Modems are devices used to convert between serial digital data and a signal suitable for transmission over a telephone line to allow devices to communicate. Modems were often used in SCADA systems to enable long-distance serial communications between MTUs and remote field devices.

The communicational level for contemporary SCADA systems is constructed in compliance with the principle of the Optical Open Transport Network (OTN).

III. SPECIFIC INDICATORS OF RELIABILITY OF SYSTEMS FOR INFORMATION TRANSMISSION

The reliability of the systems for transmission of information (including SCADA systems) has to be evaluated by specific indicators, in addition to the general technical reliability indicators. This is required by their structure and by the necessity of time reserve for processing and transfer of the information. These systems are often multifunctional and have complex hierarchical structure. This is why a big part of failures is partial and does not lead to the failure of the whole system, but only of part of it [2 – 5]. The presence of a time reserve leads to the fact that not all failures and accidents lead to failure of the functioning of the whole system, thus the term “reliability of operation” must be considered.

Probability of successful execution of the task can be used as an indicator of the system reliability if there is a reserve of time to process and transmit information. The execution of the task requires a certain time t_{task} within the acceptable range – the allowed time t_{all} (i.e. $t_{task} \leq t_{all}$). There are two options for the system operation and the corresponding indicators of reliability of operation:

1) Failures of functioning do not occur in the following cases:

- There is no loss of information when system failure occurs, i.e. the system work continues after restoration in the failure point. The compliance with the condition $t_{task} \leq t_{all}$ is needed for the successful solution of the problem.
- There is a complete loss of information when system failure occurs, i.e. the system work continues from beginning after restoration. In this case, a trouble-free operation for a time greater than t_{task} over time t_{all} is required.

Indicators of reliability are the probability of occurrence of these events.

2) Another situation arises when failures of system elements do not lead immediately to a failure of its functioning, and there is any particular or occasional time reserve for development of the failure. This kind of situations occurs in the following cases:

- Inertial objects are controlled (interruptions of the object control are allowed for a while). Indicator of reliability is the probability of execution of the control task.
- Not urgent messages are transmitted. Indicator of reliability is the cumulative time of the message retention because of a failure. This cumulative time depends on the recovery time and whether the channel is busy.

The time delay t_d because of one failure can be calculated by the equation:

$$t_d = \frac{k}{(1-k)} \frac{\tau_r}{t_m} (\tau_r - t_m), \tag{1}$$

where τ_r is the recovery time,

t_m – time for transmission of one message,

k – part of time to occupy the communication channel for transmission of one message

In most cases the following presumption can be assumed:

$$t_m \ll \tau_r \tag{2}$$

Therefore:

$$t_d \sim \alpha . \tau_r^2, \tag{3}$$

where

$$\alpha = \frac{k}{(1-k).t_m} \tag{4}$$

The recovery time generally is a random variable with mathematical expectation T_r and dispersion D_r. Then the cumulative time delay T_d because of one failure is equal to:

$$T_d = \alpha . (T_r^2 + D_r\ ). \tag{5}$$

The average cumulative time message delay $T_{d\text{-}av}$ can be calculated by the formula:

$$T_{d-av} = \alpha . \omega . (T_r^2 + D_r). \tag{6}$$

where ω is a parameter of the failures flow.

Under an exponential distribution of the recovery time $D_r = T_r^2$. Therefore

$$T_{d-av} = 2 . \alpha . \omega . T_r^2 . \tag{7}$$

The maximum value of the time delay assessment can be calculated by the equation (7), because the exponential distribution has the biggest dispersion.

The reliability of multifunctional information transmission systems can be assessed either by the execution of individual functions or by the whole system. There are two borderline cases:

1) The system provides performance of closely interconnected processes, then the failure of any one function leads to violation of all processes and the system reliability can be assessed as a standalone system.

2) The system performs quite poorly interconnected functions. If all the functions are equally important, reliability

can be estimated by mathematical expectation of the number of dysfunctions. A disadvantage of this indicator is that the simultaneous failure of several elements leads to disturbing the performance of several functions, which can lead to disproportionately heavier consequences.

The coefficient of keeping the effectiveness can be used as a general reliability indicator of multifunctional information transmission systems - it characterizes the impact of system reliability on its technical efficiency [4]. It is the ratio of the index of technical efficiency at real reliability to the maximum possible value of this indicator at absolute system reliability.

IV. INCREASING THE COMMUNICATION LEVEL RELIABILITY BY OTN

OTN is a digital communication network for real-time and mission-critical applications [2-7]. Basically, OTN is a communication backbone built up by nodes which are interconnected by a double optical fiber ring (primary and secondary rings). The transmission of signals in optical fiber instead of copper wire has several advantages: less weight and size, larger information capacity, absence of electrical connections and circuits, higher protection of the information transmitted. There is no electromagnetic interference, it is cheaper. The larger bandwidth allows transmitting all types of information on a single network. Typical communication requirements are speech (audio), computer data, LAN info, control information, video, etc. [6, 7]

OTN network architecture is based on four major system components: the fiber optic backbone, the OTN nodes, the interface cards that provide the user access to the system and the network management system (Network Control Center NCC or OTN Management System OMS). The configuration of the OTN node is influenced by the transmission medium, the distance between nodes and the topology. Different types of fiber can be used for OTN: multimode fibers 62.5/125 μm, 50/125 μm or 100/140 μm or single mode fiber 9/125 μm. Multimode fiber optic connectors are much cheaper (purchase and installation) than single mode ones. The available bandwidth x length product of multimode fiber is more than sufficient for short to medium inter-node distances with many connectors on the way. The bandwidth version also influences the choice of the fiber type. For longer distances, the only option available is single mode fiber. Here, dispersion characteristics and the overall attenuation of the fiber are the dictating parameters.

The time required by a message to travel from the transmitter to the receiver is determined by:

a. The OTN basic delay (ring delay) T_{RDb}, i.e. the run-through times of the fiber, the TRMs (Transceiver Modules), and DRAs (Dual Ring Adapters) or BORAs (Broadband Optical Ring Adapters).

b. The delay on the interface cards themselves.

The OTN basic delay T_{RD} can be calculated as follows:

$$T_{RDb} = n.t_N + L.t_L, \qquad (8)$$

where: n is the number of nodes in the ring,

t_N – the node delay,

L – fiber length in km (for a ring with loopback, also the part along the secondary ring must be considered),

t_L = 5 μs/km – the run-through time of the fiber.

The node delay may adopt the following values:

t_N = 2.2 μs for nodes OTN-2500,

t_N = 2.6 μs for nodes OTN-600 and

t_N = 2.9 μs for nodes OTN-150 at a ring with loopback and

t_N = 1.2 μs for nodes OTN-2500,

t_N = 1.6 μs for nodes OTN-600 and

t_N = 1.9 μs for nodes OTN-150 at a ring without loopback.

Newer version OTN-X3M is based on “Node add/drop bandwidth” technology and the node delay time is less than defined above values.

Communication between OTN nodes on the ring is based on Time Division Multiplexing (TDM). This access scheme allows multiple users on the ring, sharing the transmission medium. With TDM, the time continuum is divided into repetitive periods called frames. These frames are subdivided into time slots. In OTN, all time slots are one bit long. Devices can communicate when they are allocated a number of time slots during which they can transmit signals. TDM-frames are circulating on both the primary and the secondary ring at an overall rate of 147.456 Mbps, 589.824 Mbps or 2488 Mbps. These frames have a length of 31.25 μs and contain 4608 bits, 18432 bits or 73728 bits for OTN-150, OTN-600 and OTN-2500 respectively. "Channels" and "bits per frame" are equivalent for OTN.

The fact that always a whole number of frames circulates on the ring is not considered in the Eq. (8) due to the extra delay in the master node’s DRA or BORA. Subsequently, the ring delay is always exceeding or equal to T_{RDb}, and equal to:

$$T_{RD} = 62.5\ \mu s + m31.25\ \mu s \qquad (9)$$

where m is the frame number (this a whole number exceeding or equal to 0). The complete ring delay T_{RD} is considered, where the complete and possibly looped-back ring is run through once, without any interface cards.

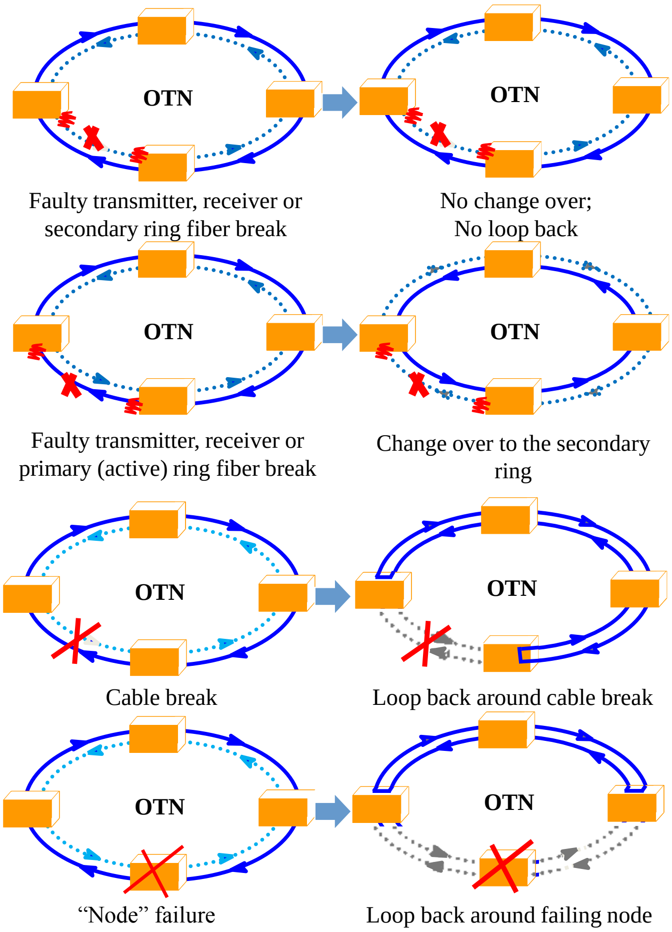
Comparing Eq. (9) and Eq. (7) it can be noted that OTN offers very high performance.

Because of the double ring structure, OTN guarantees an unparalleled degree of reliability. Should one fiber ring or node fails because of any reason (fire, rupture etc.), then the other ring and nodes take over immediately, thus keeping the whole network operational round the clock (Fig. 2).

The system will always find a way around any problem without affecting its users. The OTN nodes also offer redundancy of the main components such as power supplies, common logic cards and optical modules. Therefore, a section failure does not lead to system failure.

There are many SCADA systems in Bulgaria, which are functioning especially in very important spheres as transport and energetics. A contemporary and efficient SCADA-system is in operation in the metropolitan – Sofia and covers all of the technological processes [8, 9].

It consists of several independent systems, the most important of which are the system for operational dispatching on the train traffic DISIM-V and this one for monitoring and control on electrical equipment and traction substations DISIM-E.



Faulty transmitter, receiver or secondary ring fiber break

No change over; No loop back

Faulty transmitter, receiver or primary (active) ring fiber break

Change over to the secondary ring

Cable break

Loop back around cable break

“Node” failure

Loop back around failing node

Fig. 2. Reconfiguration

The communication level on the first metro line comprises a pair of modems, 4-wire line connectivity and an expandable system for serial communication ports (Equinox), which supports connection to a central computer in the CDP through a standard protocol and to the devices on the physical level through asynchronous protocol for data transmission.

The communication level on the newer second line is based on the optical OTN.

The newest SCADA systems in Bulgarian railway transport are also constructed in compliance with the principle of the Optical OTN [10]. They have been designed and constructed in Plovdiv-Svilengrad section of European Corridors IV & IX.

OTN offers the best opportunity for SCADA-systems in electric distribution and transmission networks. In view of the existing different kind of grid infrastructures, there are several innovative concepts for substation automation, which allows consumers to swiftly adapt the electric power system to the new conditions at present and in the future [11, 12].

V. CONCLUSION

SCADA systems are usually designed to be fault-tolerant systems with significant redundancy built into the system architecture. The system reliability can be remarkably increased by implementing optical OTNs which transfer all available communication applications, data, voice, digital video etc. and provides Accident Prevention. The environment that is ideally suited for OTN is an environment characterized by a multitude of data/ LAN/ voice/ Video communication services, distributed throughout a large area. The high availability of the OTN system is a key asset. The higher the criteria (mixed/distance) for a particular application, the better the OTN system is suited

REFERENCES

[1] Stouffer K., J. Falco, K. Kent, „Guide to Supervisory Control and Data Acquisition (SCADA), and Industrial Control Systems Security”, NIST, Gaithersburg, 2011

[2] Goranov, E., E. Dimitrova. *Remote Control and Management Systems in Transport*, Todor Kableshkov University of Transport, Sofia, 2010

[3] Clarke G., D.Reynders, E.Wright, *Practical Modern SCADA Protocols*, Newness, ISBN: 978-0-7506-5799-0, 2004

[4] Simankov V., P. Sundeev, System analysis of the functional stability of mission-critical information systems, Krasnodar, 2003

[5] Sokolov B. The optimal structure reconfiguration control in an intelligent system. Int. Sc. Conf., Pskov, 2008

[6] OTN systems – structure, features, advantages, OTN Systems, 2011, available at: http://www.otnsystems.com/

[7] OTN Systems – Dedicated Networks for Critical Environments. Available on http://www.otn.be/

[8] Technical documentation of SCADA-system DISIM-V, 2012

[9] Technical documentation of SCADA-system DISIM-E, 2012

[10] Plovdiv-Svilengrad Railway Electrification & Upgrading of Corridors IV & IX Signalling, Telecommunication and SCADA Systems for the whole line, Thales–Alcatel-Lucent, Sofia, 2011

[11] Martin, C., Lalanda, P., Donsez, D.: A MDE Approach for Power Distribution Service Development. 3rd International Conference on Service Oriented Computing, LNCS 3826, 2005

[12] System automation in substation, available at: http://www.roconbg.com/en/engineering-services/system-automation-in-substation-12