Archives of
Transport System
Telematics

Volume 2

Issue 2

May 2009

Network safety in railroad traffic control systems

S.SURMA
Faculty of Transport, Silesian University of Technology, Krasinskiego 8/201, 40-019 Katowice, Poland
EMAIL: szymon.surma@polsl.pl

ABSTRACT

This article presents the problem of safety of transmission in complex railroad traffic control systems. Modern solutions used in railroad traffic control allow for using all current means of transmission. The need to secure such transmissions is a complex issue in need of constant revision.

KEYWORDS: SIL, PLC, Ethernet, Powerlink

1. Introduction

Traffic control system in currently used applications consists of a superior control device and executive devices. Executive devices are merely mediating in information gathering and controlling the transmitters that constitute current outputs. The software for these devices includes just the security features, such as displaying the red light when communication with the superior computer is lost or an emergency situation arises (such as a burned bulb). The concept of decentralised systems relies on assigning some basic algorithms to peripheral drivers, in order to accelerate the reaction when transmission between the driver and the superior computer is lost, and to relieve the central computer.

Solutions based on PLC drivers are currently used in secondary German railroads, where SIL 2 (safety integrity level) is required, while the parameters of railroad traffic are limited. These are mainly commuter and regional trains (according to internal German railroad regulations). It is a starting point for using PLC drivers in applications with SIL4 safety, as the drivers themselves can satisfy SIL4 requirements, yet they do not have to when combines with software.

Issued described herein will relate to the possibility of using integrated programming environments to build software for decentralised railroad traffic control systems and to secure the network infrastructure against interference from unauthorised people.

2. Decentralised system

The idea behind this system is to decentralise data-gathering devices and partially decentralise the superior layer of management. The concept of layered system is based on SCADA systems, but limitations had to be introduced to the starting assumptions for security purposes. Example diagram of system structure is presented in fig. 1.

Current systems have only used drivers as elements of information-gathering and executive layer. The possibility to install on-site devices, that would be responsible for security control, or even replicating the functions in various devices located at some distance from each other allows for increased reliability of superior layer without increasing the cost of system installation and operation. Elements from two layers can be implemented in every PLC driver in the system: decisive, and data-gathering and excutive. For reasons of economy and security of such solution, two possibilities should be considered – implementing the decision layer as a separate hardware and logic level or as a combination of decision and executive level.

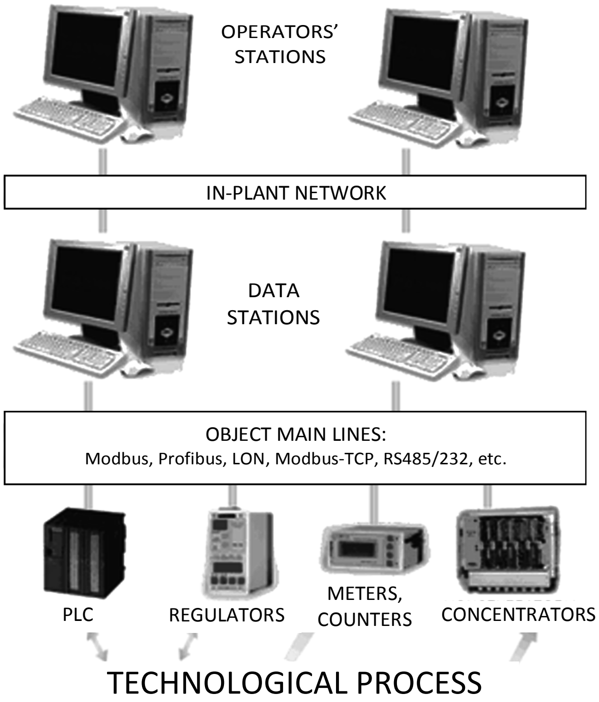

Fig. 1. Layered structure of SCADA system
Source: [10]

In the traditional software development process, decentralising the superior layer increases the complexity of system structure, thus increasing its cost. Using a centralised programming environment for developing the whole system reduces the development cost by increasing the level of integration of software and communication layers. Software development process in an integrated environment is not based merely on code-processing, but mainly on graphical compiling of logical connections between individual blocks, representing devices or their elements. Thus, software complexity can increase development cost only when using current development methods. Software development for all devices and system layers in one programming application/environment, which integrates all system elements allows for introducing new functions to system elements without the loss of its integrity and security.

The security of these solutions should be considered in two directions. Firstly, one should consider security of the software that will be expanded when functions from the superior layer are implemented in the PLC drivers. According to programming environments' principles and PN-EN 61131 standards, they will certified blocks, whose code will be written, verified, tested and validated just once. It is possible to implement in the code of individual blocks the elements, that would test their correct operation, and to add diagnostic blocks to developed applications.

Second security issue has to do with the communication infrastructure between the central computer and drivers. Regardless of the level of independence of superior blocks in drivers, loss of communication between the computer and driver has to cause the driver to enter safe mode, i.e. to display the stop signals on semaphores and wait until normal transmission is restored. Even though it would be possible to automatically operate given area by dependencies included in driver software, the lack of data recording on central computer, as well as lack of supervision by the train dispatcher, would lead to dangerous situations. Local control using a portable operating panel can be implemented as an additional functionality of decentralised system. In case of a communication failure, the dispatcher (assistant) can be appointed to control part of the station an manage traffic in given area by giving special orders.

3. Communication security

Security of communication between PLC drivers and the central computer can be divided into medium security and transmission security. Depending on the location of individual elements of the system, security assurance for the medium can be hard to implement. Lack of interference in the medium should be ensured, meaning physical breakage, signal interference and transmission interference by transmitting signals or listening to them. Implementing such principles would require vast investments, which makes this solution considerably less applicable.

Security reaction in transmission does not decrease security level, but it may result in decreased system readiness level due to the activities caused by lack of communication. This is one of the most important drawback of a system with guaranteed transmission security, as frequent interference resulting in lack of communication between objects may cause total lack of system readiness.

Transmission security is guaranteed by controlling its correctness and transmission encryption. Transmission correctness control is done based on package checksum (hash) control on both sender and receiver ends. Changing one bit of data causes the checksum to change, and the package is ignored. There is a possibility of conformity of two checksums for different packets, provided that there is a difference on given number of bits. Identification of incorrect packet as a correct one is occurs with certain probability, which is converted to the probability of not detecting a mistake for the same message sent with given

$$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x+1$$

Fig. 2. CRC32 polynomial according to IEEE 802.3
Source: [10]

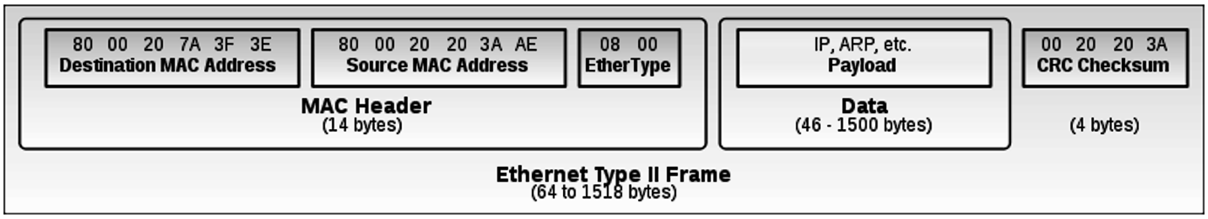

Fig.3. Ethernet transmission frame.
Source: [1]

Hamming Distance (HD) [[Philip Koopman: 32-Bit Cyclic Redundancy Codes for Internet Applications The International Conference on Dependable Systems and Networks (DSN) 2002]. For 32-bit CRC (cyclic redundancy code) and MTU (Maximum Transmission Unit) of 1500, the level of transmission error detection is at the detection probability level of HD 5. fig. 3 presents Ethernet frame structure.

PN-EN 50159-2 standard does not regulate the requirement for HD value, but it considers CRC-only security as insufficient and requires using other transmission correctness testing system in open systems. It has to be noted, that open systems, that do not use universally accessible computer networks, have a maximum security level of 4 (level 4 defines railroad WAN, while it is not equivalent to SIL level), which allows for disregarding transmission errors caused by men (hackers). Such approach allows us to concentrate on ensuring the correctness of transmission and not on its protection. Checking transmission correctness is also possible by using encryption, which can now be implemented in every element of control system based on PLC drivers.

Requirements for both open and closed systems according to PN-EN 50159-1 and PN-EN 50159-2 explicitly define the need to separate secure and insecure transmissions for identification purposes. Transmission encryption with one transmission channel was given in the standard as one of the solutions for open systems. It is a compromise between expenditures on additional medium for secure transmission and separate one for insecure transmission, while ensuring additional security against unauthorised access.

3.1. Wireless transmission

Wireless transmission systems are not prohibited, and even referred to in standards [50159] as one of the solutions. While radio communication systems as a medium can be regarded as safe now, the progress in cracking the cryptographic safety measures may give rise to fears, that such systems will not be considered safe in the future. Railroad computer system's lifespan is at least 10 years. In the last decade, WEP (Wired Equivalent Privacy) encryption was cracked, and now an attack retrieving the encryption key takes less than one minute [2][3], as proven by the scientists at the Technical University of Darmstadt. Current works, by the same university, on cracking WPA (WiFi Protected Access), which has been considered safe so far, has proven that TKIP (Temporal Key Integrity Protocol) encryption is not fully safe. In article [4], E. Tews cites the need to change corporate network encryption from TKIP to AES (Advanced Encryption System), which is a hint, that planned implementations based on encryption should include at least one AES method with a 128-bit key. Transmission security and reliability can be enhanced by double encryption - first by the system, and then by the transmission device. Such solution will ensure that messages concerning the insecure part of transmission will also be encrypted.

In case of wireless systems, apart from the risk of break-in (wiretapping or distortion), the level of interference caused by other users of the same waveband, as well as external factors, can also have noticeable influence. These factors are impossible to eliminate (a licensed frequency can be used, but this will increase the cost of building and operating the system). There are serious reasons not to use radio transmission: possible break-ins, interference, susceptibility to unauthorised usage. Radio transmission should therefore be used as a last resort.

It should also be reminded, that there are wireless solutions far less vulnerable to unauthorised access. Optical communication, which uses laser as a medium, is one such solution. It has its pros and cons compared to radio transmission. The main drawback, but also the main an advantage, it the angle of view of the source and receiver, which can be less than 1 degree (in radio transmission (WiFi), the signal is broadcasted around the source, while maximum signal power is achieved within less than 1 degree), and there has to be optical visibility, which is not always required in radio transmission and depends on signal power and quality in receiver. An obstacle between the source and receiver will break the transmission, which can be limited to breaking the transmission only by passing birds, if set up correctly. The effect of fog on transmission is a much bigger problem. A fog, which limits the visibility below 6% of the distance between the transmitter and receiver (60m for 1000m) causes the transmission to break. For laser transmission, transmission error level is as low as 10-9 [5][6], which in case of radio transmission depends on momentary electromagnetic interference, even from distant sources concurrent with the signal beam.

Interference, both created by an attempt to break in and by

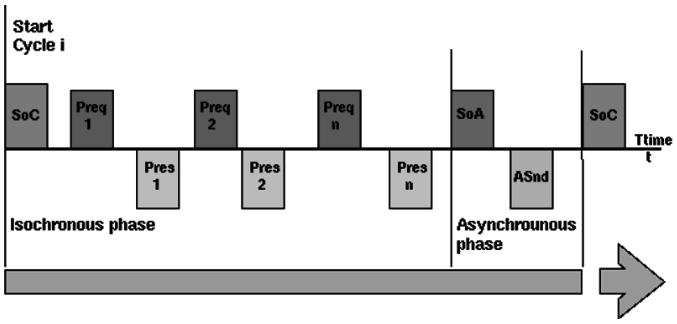

Fig. 2. Combination of isochronous and asynchronous transmissions in POWERLINK protocol
Source: [8]

external sources (electromagnetic field, lack of contact), results in the need to set up a connection again. Such operation occurs in both wireless and wired transmission and is connected to the principle of Ethernet physical layer, as well as the principle of CSMA/CD access.

4. Used transmission protocols

In industrial networks, PROFIBUS is now the most widely used protocol. The main difference between this protocol and Ethernet are lower speed to distance ratio stemming from the physical layer of Profius protocol i.e. RS485 standard [7].

Ethernet-based solutions, such as Powerlink Ethernet or Profinet, allow for transmission over standard Ethernet cables, while retaining security level and increasing transmission rate. Lack of need for hardware reconfiguration increases system flexibility and allows for implementing partial functionality during system modernisation or rebuilding. The transmission protocol selection is practically dependent on hardware manufacturer.

In order to ensure proper security level and quick reaction to system changes, Powerlink Ethernet transmission frames are built differently from standard Ethernet. This change is to ensure prioritising transmitted information. The central unit, which controls network operation (allowing to use the medium) assigns medium access rights during isochronous transmission. After this, asynchronous transmission occurs, during which the standard CSMA/CD-based model can be used. This allows for connecting a new device at any place and, with proper configuration, using it in the control process. Additionally, the real-time network should be separated from the unsafe network using software and hardware-software tools. [9].

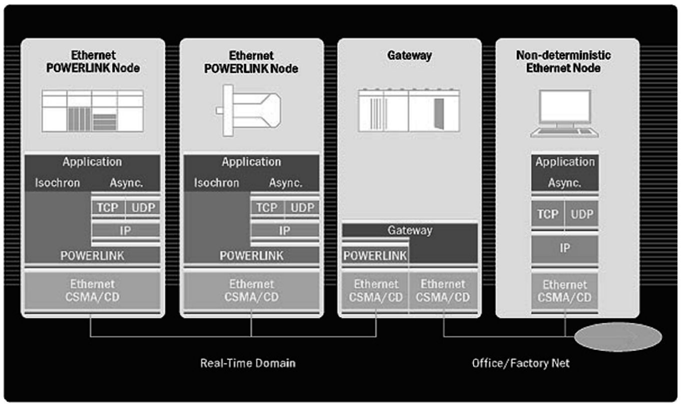

Fig. 3. Complete separation of real-time network by POWERLINK.
Source: [9]

5. Conclusions

In the last few years, the changes in transmission and encryption systems allow for using open protocols in industrial applications. Universal access to documentation does not diminish system security. Safety should be guaranteed not by keeping the system documentation classified, but by a policy of security and access restriction, i.e. passwords, keys and access rights.

Using open software to build control systems may improve system familiarity of new employees and introduce new approaches to developed or existing systems, both in construction and in security. Using closed products results in the need to fully train every employee who is supposed to work on developing the system, which is expensive and time-consuming in most cases. Additionally, it should be noted, that a fan of given development method will be far more effective than a person forced to work in a given way, which is another argument for using open and widely used programming languages and protocols.

Bibliography

[1] http://en.wikipedia.org/

[2] http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/

[3] http://eprint.iacr.org/2007/120.pdf (2009-05-10)

[4] http://arstechnica.com/security/news/2008/11/wpa-cracked.ars

[5] LaserBit LB-2500 Modular Series Documentation, http://www.cyberbajt.pl/download/laserbit/dokumentacja/LB-2500_Data_Sheet.pdf

[6] TereScope155 Protocol Independent Series, http://www.mrv.com/datasheets/TS/PDF300/MRV-TS-007_HI.pdf

[7] http://www.profibus.com/pb/profibus/process/

[8] http://en.wikipedia.org/wiki/File:Epl_cycle-3.png; user Plupp01

[9] http://www.ethernet-powerlink.org/index.php?id=40

[10] ZEiSAP MikroB S.A.