Railway Security Issues: A Survey of Developing Railway Technology

Albert H. CARLSON
Computer Science Department, University of Idaho
Moscow, ID 83844

and

Dr. Deborah FRINCKE
Computer Science Department, Center for Secure and Dependable Systems, University of Idaho
Moscow, ID 83844

and

Marc J. LAUDE
Computer Science Department, University of Idaho
Moscow, ID 83844

ABSTRACT

Transportation systems are increasingly under scrutiny with respect to potential vulnerabilities. As part of the National Strategy to Secure Cyberspace [19], threats and vulnerabilities to cyberspace are being identified and remediated. Primarily the discussion has focused on physical security or the security of those systems that are well known to be heavily dependent upon electronics, such as avionic systems. Transportations systems such as cars, trucks, and trains are not as frequently considered. Consists[1] are engineered for comfort and customer satisfaction, often employing the most accepted technologies. Rail manufacturers and properties in the United States often follow that lead and are presently fielding systems that are based on microprocessor and integrated electronics technology [18]. This paper explores the state of security and possible problems in the rail infrastructure, including susceptibilities to internet technologies.

Keywords: Railway, railroad, transportation, network security, security, hardware

INTRODUCTION

Railways have been a means of commercial transportation for both passengers and freight since 1825. During the intervening years, a variety of cutting edge technologies have been used. Generation of electricity on the trains through Head End Power (HEP), or transference of power from a local power grid accessed by the train through Third Rail or Catenary sources, made lights, environmental systems, and remote actions – such as opening and closing doors for passengers – possible. Radio made communications with trains in remote locations possible and systems on the trains were able to communicate on a limited basis through trainlines (Figure 1). Due to the size of the electrical equipment, complicated and complex circuitry was far too large to be located on the train consists. As electrical equipment became integrated, the size of components shrunk, making consist wide and train wide communications possible for control systems and for communications with data based elements, such as computer systems and the Internet. While train wide and car wide small networks brought with them increased capabilities, they also bring with them the vulnerabilities associated with integration of networks in other areas [1]. Rail systems should be considered likely targets for attack – their management is somewhat obscure and their disruption leads to the potential to create chaos. The question is: "How well are rail systems protected?" Secondarily it must be asked, "What has been done to this point to secure a vital link in the infrastructure and where will the trends to integrate even greater levels of technology make rail systems vulnerable?"

THE DEVELOPMENT OF ELECTRICAL RAILWAY EQUIPMENT

Railways have been a mainstay of transportation since the mid 1800's, both in the United States and in Europe. This trend continued in the United States until the mass availability of the automobile and a reliable intercontinental road system. In Europe, the movement to automobiles never happened as it did in the United States. There was no large-scale move away from trains and public transportation. Europe continued to build their rail infrastructure. With rising oil prices and shortages, there has been a return to rail service in the United States. This includes more long haul service by rail instead of truck and light rail for commuters.

Early rail control was all mechanical in nature. Men ran across the top of railcars to apply brakes, manipulated levels in towers to operate track switches, protected rail crossings, and every engine had a crew. To increase profits people were required to

[1] Consists are rail cars placed together in a specific order, or a train formation, excluding the locomotive. [17]

do more, air brakes were developed, getting men off the top of cars and allowing for longer, faster trains. With the availability of electricity in the later third of the 19th century, more mechanical systems were upgraded and changed to electrical control. Mechanical switch towers were phased out, signaling was installed, diesels replaced steam and radio communications replaced telegraph and notes. The timeline of these advances and those following are shown in Figure 2.

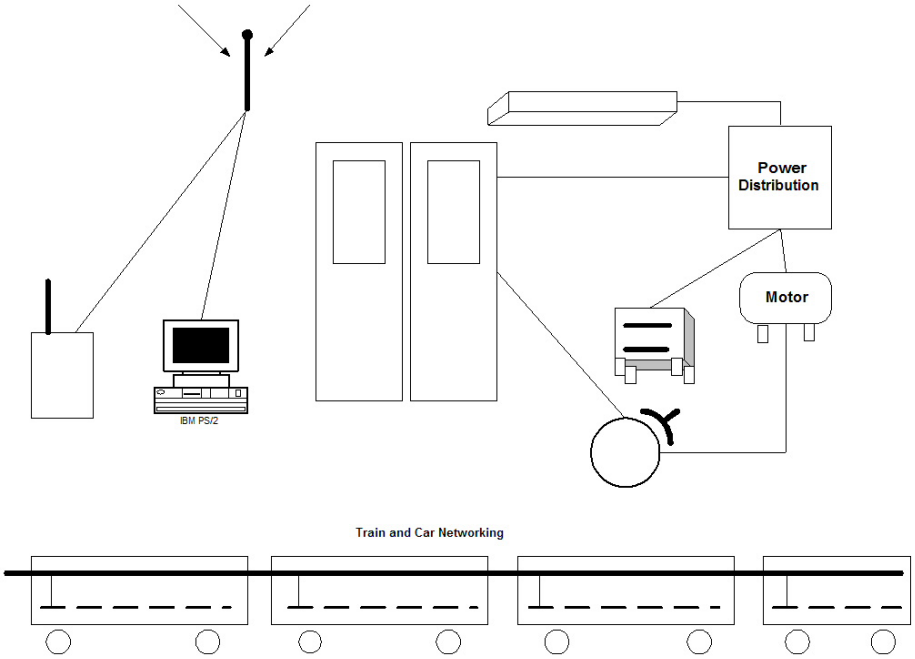

Figure 1 Rail Network Composition

Electrical equipment continues to be used today. Electronics [14, 15] brings the power to do many tasks with a small penalty in space, power and time. Microprocessors have proven themselves as a mainstay of equipment required to automate functions not requiring human intervention or decision making. It was inevitable that rail technology would eventually integrate these advantages on-board [6] and make computers a part of the arsenal of rail equipment. The Dash-2 series from General Electric, for instance, introduced microprocessor control into trains. Microprocessor control systems have allowed for smaller two men or single man crews. Computers allow programming to restructure tasks as needed and can integrate data from sensors to perform or modify their task in reaction to changing or variable physical conditions

Nieva et al., Sullivan, and Chen all agree on the direction in which rail equipment is headed, though each set of authors concentrate on different areas of equipment development. Both sets of papers indicate that once a computer was placed in the train that software techniques would have to keep pace with the industry. Sullivan [13] chronicled the history of electronic and argues that integration that has lagged behind the rest of the industrial sector is bound to come, then in a later paper that it has arrived in the form of a network-like control bus for rail [14, 15]. While Sullivan concentrates largely on the system as a whole, concerning himself with the hardware as well as the software, Nieva et al. and Chen have concentrated on software.

Nieva [10] notes that the transition to integrated electronics has necessitated both a change in hardware and in software, working with distributed objects that he assumes will be available on all newer train platforms following design standards. They, along with Chen and Fokkink [2, 7] share the same basic assumption of capabilities being built in now and in the future. However, unlike Sullivan, they take this integration one step further and extend it into the critical maintenance and planning infrastructure behind the operation of the train. For instance, Chen is concerned with the use of a distributed system to coordinate the use of the train in sections of a system so that loss of one sector does not take down the entire line. Fokkink is concerned with the representation of data and how to use the mathematical model to coordinate safety in routing and signaling in the rail station. Both seek to use a distributed methodology to express how trains operate and prove that it is possible to schedule a train through a section of track using these concepts. This also includes the coordination of monitors set along the track to sense the state of the equipment in the area and communicate back the state of the track. Nieva et al. discusses how to coordinate remote monitoring of a train

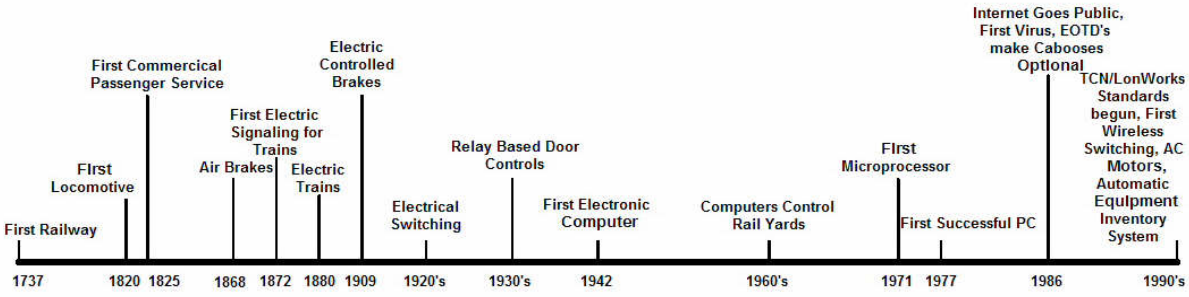

Figure 2 Railway and Electronic Equipment Timeline

[6, 11] as well as how to use internet technologies to work with the train in a station to download and upload information, answer database queries, and coordinate maintenance from a train gateway in a station.

The IEEE has also recognized the movement of control systems in this arena to become integrated and shows them as a network of importance. Two specifications have been widely accepted in the United States for use in the communications of data along a train network. These are the IEEE 1473-L and –T standards [14]. Along with these coordinating standards are others specifically aimed at rail applications [18]. Clearly this indicates that the movement to standardized network communications is happening.

SAFETY CRITICAL CIRCUITRY

Systems inside the train are denoted as "safety critical" if they can cause great damage to persons or property [3]. These systems include, but are not limited to doors, brakes, propulsion, environment, power distribution, and communications, and lighting [6]. Each plays a vital role in the operation of a train and most are interconnected. For instance, the doors in a passenger rail train are typically connected to, and directly influence, the braking and propulsion of a train. Some of the systems, such as doors, lighting, and environment are typically associated with passenger rail service, although they are also applicable to a lesser extent in freight systems. In this section, we discuss several safety critical aspects of railway.

CRITICAL RAILWAY SYSTEMS

The braking system on a train is one of the easiest to imagine as a safety critical system. Once underway, trains represent a repository of momentum that is hard to stop in a short space. Engines alone can weigh over 180,000 lbs [4, 9] and can travel upwards of one hundred ten miles an hour. Some coal trains stretch over two miles – with newer braking systems allowing lengths of up to three miles – and are fully loaded with coal weighing hundreds of tons [15]. Obviously, brakes that fail can result in tragedy. When traveling too fast and encountering a curve the train may derail, allowing the train to enter areas where it was not designed to travel and to strike structures or persons not normally expecting the presence of a vehicle of that size. Numerous examples also exist where trains have been involved with other vehicles at crossings, striking them and resulting in injury and death [8].

Propulsion of the train, and the control of speed, is another critical system. The velocity of a train must match the rail conditions if the train is to stay on the tracks. Trains must also not be allowed to move when it is inappropriate. Failure to move, or to be able to move at the right time may result in train collisions, derailment, or striking objects in the path of the vehicle.

Doors are a very important system that is often not recognized for the impact it has on train movement. They allow passengers to enter and exit a train only when appropriate. Opening or closing the doors at the wrong time may allow passengers to exit or fall from the train, or alternately, closing the doors may trap passengers between them, resulting in injury. They are also closely connected to the brakes to ensure that the train cannot move when they are open. For this reason, the door system is of particular interest to an intruder attempting to prevent train movement.

The environmental system is normally used for passenger comfort. However, when the external temperature is at either low or high extremes, sickness and death may result. Sickness may take the form of heat prostration or freezing and can span a wide range of symptoms. Freight also relies on environmental controls, as it can be potentially damaged from excesses, resulting in loss of revenue for both the shipper and the shipping line. Perishables must be kept cold to preserve them during transportation. Food is especially susceptible, but there is other cargo that also reacts badly to a temperature range that is inappropriate. Electronics and other sensitive equipment must be kept within specified storage temperatures, for example. If stored and/or transported using an incorrect environmental setting damage or destruction will result.

Communications and signaling are also critical systems. Engineers and train crews must know what is ahead of them in order to guide the train correctly. Topographical features, as well as train routing, may make it impossible to see far enough ahead to avoid collisions. Good communications, signaling, and routing allow crews to react to changing conditions to avoid collisions, accidents, and other hazards.

RAILWAY CIRCUIT VULNERABILITIES

Recent discussion of networking on rail platforms [10, 15] indicates the potential for tremendous gain when trains can be networked to services provided by applications at remote locations. Nieva et al. discussed passenger comfort [6] as well as the ability to download data on the passenger or freight manifest. Fokkink [7] brings up the coordination possible to route and control train movements with signaling and routing equipment. Nieva et al. [10] note that information can be passed to and from the train to ease coordination of passengers and freight, as well as maintenance. Nieva et al. [6, 11], Fokkink [7], and Chen [2] work with remote monitoring and planning for trains as an improvement over present service.

Many of the suggestions for improvements include wireless connections [3, 6, 15] to make it possible to easily maintain communications with a mobile platform – in this case, the train. Nieva et al., also suggest the medium of wire in passenger trains where large amounts of data are transferred very quickly [10] and where it is critical that data be transferred correctly. The JINI system implementation explored by Nieva et al. is just such a system, wire based to a stationary passenger train employing Ethernet-like, if not Ethernet, communications to talk with the train.

Although making use of basically the same communications methods, the actual communications implementation to and from trains varies. Presently, one of the more important projects in inter-train communications is the consolidation of drivers (Gateways) for implementations of the IEEE 1473 type systems [15]. IEEE 1473-L, LonWorks [5] and IEEE 1473-T, Train Control Network, based on the European ROSIN definition [6], cannot talk to each other over a direct link. This means that trains made up of consists produced by different manufacturers using different train control network standards are not able to communicate. Gateways are needed to provide for

communications between TCN and LonWorks equipment, but are not yet in place. Both standards have control networks, and both integrate data communications. Though not explicitly stated, both standards have functionality that suggests that the communications networks are directly connected with the control system. Remote monitoring suggested in all cited papers of this type [2, 6, 10, 13] indicate that the explicit separation of the networks was not accomplished. All papers specify the use of wireless communications protocols, specifically those based on IEEE 802.11x standards for communications. The TCN network also implements a wire transfer mechanism through the Train Gateway. This practice represents a possible security vulnerability. IEEE 802.11b WEP standards, to date, have well documented and exploitable security flaws [15]. Wireless can also be taken over by a more powerful signal, resulting in loss of communications and control. Any time control is mixed on the same network with communications, there is a chance that the messages to the control mechanisms can be faked by an intruder, generically known as "spoofing." Further, internet like technologies are susceptible to the same kinds of network attacks as the internet itself. These include the possibility of infection by viruses, worms, and related software. While Java appears to be the language of choice in some TCN implementations [6, 10], Java viruses are known and documented [16]. These vulnerabilities indicate that trains involving networks may be vulnerable to attack just as common networks are.

Mobile networks are not the only target for malicious attacks. Transit companies must sell tickets, assign seats, keep maintenance records, and plan for personnel and equipment assignment. These also are vulnerable to attack. Freight hauling properties have similar vulnerabilities in their manifest, routing, transfer, and storage location software. A cracker intruding on the system could reroute cargo, change the description of the freight, send it to a location thousands of miles from its true destination, and then have it stored in either an inappropriate place (such as an ice cream shipment not put in refrigeration) or hide it altogether. The effect of such an action would be to create chaos in the company and increase insurance claims for damaged goods. Customers would loose faith in the abilities of the rail network and shipments would decrease. The cost of returning goods to their proper location would also prove costly.

Some of the same information is present on the TCN equipped trains. Manifests can be downloaded to the train where an experienced network intruder can change information if it is not fully protected.

Standards that are now in place in the form of TCN and LonWorks do not adequately consider security given the developments brought to light by events like the September 11, 2001 attack. TCN security pins its hopes on the language in which it is implemented. In separate papers Nieva et al. explicitly state that they rely on the "secure" nature of Java. While Java does exhibit some security features, the job of keeping the Java environment secure rests squarely with the software developers. If the software design defeats these measures, the environment is compromised and the entire design becomes flawed (from a security standpoint) and insecure. Designers take the first step by selecting Java, but then they go on and intentionally move outside the sandbox with Remote Method Invocations (RMI) accesses and create a class of objects meant to ignore the sandbox [6]. Nieva et al. continue by indicating that information that is fed into the system will have a digital signature. This is, again, a good start, but it places reliance on the Trusted Third Party (TTP). Such a measure should be viewed in light of problems encountered by several TTP organizations.

Nieva et al. [10] did add further security features in the form of passwords on the station connection to the Train Gateway. Here a challenge-authentication password system is specified. All password programs are a potential vulnerability, though with the right password enforcement, this may not be a large vulnerability.

Unprotected wireless communications systems, and the media used for train communications are a source of vulnerability. As previous described, these links need to be well guarded and secured to ensure that passengers, crew and cargo remain safe.

The communications systems with trains can learn lessons from the power industry in developing their SCADA systems to use web technologies. The lessons they have learned can be leveraged in railway security. They have remote assets that can be operated or checked remotely using web technologies. Recommendations have been made for "Hardening" their networks against direct attacks, these recommendation are just as valid for railway networks. These recommendations include [12]:

1. Isolate critical controls. Use different networks for train control and passenger usages.
2. Use adequate password control and protection.
3. Make individuals accountable through protected logs. Users from engineers to maintenance/signal personnel to management to dispatchers must have unique id's and passwords to gain access to the system. Logs must be considered highly valuable and protected accordingly and track changes to the systems and system activity.

Following is a compendium of Do's and Don'ts from [12] on securing computer network systems. They are organized by usage category so relationships are more apparent.

Password Management:

- Use "hard" passwords of six or more characters with mixed case and special characters
- Don't use common words, acronyms, or personal information like birthdays, names, etc.
- Memorize passwords, don't write them down
- Change passwords periodically (the U.S. National Security Agency recommends monthly or quarterly)
- Change passwords immediately after instances of contractor installation and maintenance, suspected intrusions, and when personnel turnover or strife increases insider risk
- Use different passwords in differing locales, equipment and systems; don't be tempted by single sign-on ease of use
- Ensure that passwords are issued and controlled locally (and not widely distributed)
- Teach password security and monitor compliance
- Force periodic password change, use password checkers to identify and eliminate weak passwords

- Avoid using devices with inadequate password protection (e.g., numeric-only passwords of less than eight digits)

Alarm Events:

- Issue alarm contacts for access, password, and settings events
- Monitor alarm contacts and events diligently. Not only for intrusion detection, but to verify device functionality
- Log alarm events and suspicious activity (e.g., failed password attempts) in non-volatile memory
- Scan access logs and audit files regularly
- Automate the response to alarm conditions with preprogrammed disconnects, auto-dial warnings, and increasing audio and visual alarms

Network Connections:

- Use private communication lines when possible to limit public eavesdropping and potential intrusions
- Implement access hierarchies with different levels of permission for viewing and setting devices
- Use point-to-point star topologies (i.e., .home-run lines.) from access points to controller to increase survivability and avoid .one down, all down. vulnerabilities
- Use passwords, access restrictions, and user authentication to guard against unauthorized access
- Secure Control and IT systems with virus scanners, firewalls, and intrusion detection systems
- Limit access to communication systems design and network access information

Connectivity:

- Use warning banners. to discourage electronic intrusions and enable electronic monitoring and trespass prosecution
- Use secure dial-back, encrypting, or authenticating modems and network devices
- Terminate interactive sessions after long periods of inactivity. ensure that the open port is properly closed so the next user does not inherit unauthorized access privileges
- Limit the number of failed attempts to enter a password disconnect and time-out the communication line after a set limit

THE STATE OF RAILWAY SECURITY

Presently, electronic and network security has not been well studied, or addressed with respect to rail systems. Of the papers surveyed, only the Nieva et al. papers [6,10] addresses the subject. While disappointing, this is hardly unexpected because of the low technology image of train systems and their relative lack of popularity in the United States. There have been no known real threats or effective attacks against trains using an electronic or network vehicle. Trains have simply been off the screen as targets of crackers (hackers dedicated to causing disruption and destruction) and terrorists. Air frames make more spectacular targets, move faster, and get more press. But, sooner or later, someone, possibly in the terrorist base, will recognize the importance of rail transit and transport to the smooth operation of the United States and Europe. When that happens, attacks will start.

CONCLUSIONS

Trains are essential to the daily operation of the nation. Commuters and passengers make daily use of the trains, while tons of freight are moved daily from suppliers to consumers. Shutting down rail traffic would severely hamper movement of workers and materials all over the United States. Europe is even more dependent on rail service than the United States.

As part of the critical infrastructure of a nation, it is likely that rail systems will be rising on the threshold of interest for potential attackers. The question of which is likely to be the most attractive of freight, passenger, or unmanned as a potential target is not yet answered. One could, however, speculate that those directed against unmanned, autonomous vehicles would be more effective and have greater impact because of the lack of a crew to manually recover control of the train if an attack were to occur.

Railway security is no longer the exclusive purview of private police walking a beat in the rail yards. Since 1994 standards were put in place that requires more than just physical security. Microprocessors are used in many applications that are safety critical. Networks connect control and communications functions, making them vulnerable to the types of attacks all other networks endure. The addition of communications to a central authority, usually wireless, increases the number of ways that security can be breached and the train can be attacked. Electronics in the control path solve many problems, but also introduce additional vulnerabilities.

Control networks and communications are not the only way that rail systems can be attacked. Rail companies have placed a great deal of information on the computer in order to better service their customers. Lists of passengers, manifests and lading documents, ticketing, scheduling, routing, and signaling are also susceptible. Network security is required in order to keep this information, and the transportation of this data, safe.

A mix of physical and network security is required. To date, rail systems have not addressed this need for security, but this need must be filled in order to keep this part of the nation's critical infrastructure safe and operational.

BIBLIOGRAPHY

[1] A.Carlson, D.Frincke, and M.Laude (2003), "Railroads and the Cyber Terror Threat", **Technical Report CSDS-DF-TR-03-14**, Center for Secure and Dependable Systems, University of Idaho, 2003.

[2] Y.Chen, (1999) "Autonomous Decentralized Systems and Their Applications", **Elektron Journal of SA-IEE**, May 1999, pp. 52-55.

[3] Y.Chen, (2000) "Operating Systems for Safety Critical Applications", **Elektron Jounal of SA-IEE**, January 2000.

[4] General Motors EMD (2003), **SDM740M Product Specifications**, http://www.gmemd.com/en/locomotive/na_freight/sd70m/index.htm

[5] Echelon Corporation, (2002) **Lonworks Overview and Lontalk Protocol**. http://www.echelon.com/products/lonworks/default.htm

[6] A.Fabri, T.Nieva, and P.Umiliacchi, "Use of the Internet for Remote Train Monitoring and Control: the ROSIN Project" presented at **Rail Technology '99**, London, UK, September 7-8, 1999. http://icawww.epfl.ch/nieva/thesis/Conferences/RailTech99/article/RailTech99.

[7] W. J. Fokkink, (1996) "Safety criteria for the vital processor interlocking at Hoorn-Kersenboogerd", **Proceedings of the 5th Conference on Computers in Railways**, {COMPRAIL}'96, Part I: Railway Systems and Management", p.101-110

[8] US Department of Transportation, Federal Railroad Administration, (2001) **Railroad Safety Statistics Annual Report 2000** http://safetydata.fra.dot.gov/OfficeofSafety/forms/Default.asp?page=publications.asp

[9] How Stuff Works, Inc. (2003), **How Stuff Works – Diesel Locomotive**. http://www.howstuffworks.com/diesel-locomotive.htm

[10] T.Nieva, A.Fabri, and A.Benammour, "JINI Technology Applied to Railway Systems" **Proceedings of the 2nd International Symposium on Distributed Objects and Applications (DOA'00)**, p.251-259 http://www.computer.org/proceedings/doa/0819/0819025labs.htm

[11] T.Nieva, A.Fabri, and A. Wegmann, "Remote Monitoring of Railway Equipment Using Internet Technologies" **EPFL-DSC**, April 2001, Technical Report N° DSC/01/018

[12] P. Oman, E.O. Schweitzer III, D. Frincke, "Concerns About intrusions into Remotely Accessible Substation Controllers and SCADA Systems, 2000, **Paper #4, 27th Annual Western Protective Relay Conference**, (Oct. 23-26, Spokane, WA) http://www.selinc.com/techpprs.htm

[13] T. Sullivan, "A Revolution in Serial Trainline Communications", **Railway Age Magazine**, August 1998, Vol. 199, No. 98, p.63-74.

[14] T. Sullivan, The IEEE 1473-L Communications Protocol: Experience in Rail Transit, **APTA June 2002**, p.293 – 298. http://www.tsd.org/papers/IEEE%20201473-L%20Communications%20Protocol.pdf

[15] T. Sullivan, (2003) **Private Conversation**, Phone, February 4, 2003.

[16] Symantec Corporation (2003), **Security Response Java App. BeanHive**, Internet. http://www.symantec.com/avcenter/venc/data/javaapp.beanhive.html

[17] Trainweb (2001) "Glossary of Modern Railway Terminology", Internet. http://www.trainweb.org/railwaytechnical/newglos.html#C

[18] TSD, (2003) Train Control Suppliers http://www.tsd.org/communic.htm

[[19] US Government, National Security Office (2003) **The National Strategy to Secure Cyberspace, Internet**, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf