Protection of a Communication Based Train Control System from Hackers

Ir Henry CHEUNG, PEng CEng RPE(CAI, ENS), FIRSE FHKIE FIET SrMIEEE, IRSE Hong Kong
Mr K W Pang, FIRSE MIET, IRSE Hong Kong

SUMMARY

CBTC systems have in recent years become the industry standard solution for metro signalling. Using commercial off the shelf wired and wireless communications equipment the CBTC system faces cyber related threats similar to the computer network in other industries. This paper looks at the cyber security risks that may affect the operations of a CBTC system, the available standard and protection framework, and proposes necessary CBTC system requirements to address these risks.

1 INTRODUCTION

In recent years, Communication Based Train Control System (CBTC) has become the main stream automatic train control system (ATC) for metro systems around the world, and is gaining popularity for metro operators, asset owners and passengers. In most of the radio based CBTC system implementations, over 95% employ Wi-Fi based train-to-track communication due to the widely available hardware and ease of implementation. In addition, the operations control centre to interlocking and CBTC zone controller communication links are mostly based on the Ethernet based computer network architecture. This advancement in technology to the railway signalling industry also brings along the issue common to the Information Technology (IT) industry of unauthorized access and control by external parties.

If we look back in time, the two key significant events that transformed the thinking of the railway industry about system safety and operation safety were the Clapham Junction collision and the King's Cross fire. The investigation reports of these two accidents led to the development, amongst others, of the concept of risk based safety management and safety integrity levels for railway systems, equipment and components. Computer hackers do have the capabilities of breaking into any computer based railway system, taking control, and causing disruptions, chaos, or even accidents.

Moving forward, we must now equip our CBTC or any railway system with appropriate protection against these cyber attackers from disturbing the safe operations of trains. We will look into the various penetration mechanisms, introduction of safety measures and best practices that help to mitigate potential cyber security breaches.

2 CYBER THREATS

2.1 Cyber Security – What is it Anyways

The existence of thieves and robbers could be dated back to the dawn of civilization – when there was anything worth something, someone would try to take it from its rightful owners. In the world of IT, we are able to identify similar behaviour. In the age of information, everything we own is converted into a sequence of 1's and 0's and is stored electronically in the virtual world of internet. Our centuries old nemesis, the Voldemort of Information Age, the thieves of the network world, the black hat hackers. According to Cisco, cyber security is a practice to protect computer systems, networks and software from unwarranted access by a third party. The aim of such acts are for personal gains, or malicious deeds.

Before the popularity of smartphones, people often saw cybersecurity as a problem only applicable to large corporations such as financial institutions, government agencies, or large corporations. In recent years, with smartphones being common with more than 5 billion of the 7.7 billion people in the world having a mobile subscription of sorts, cyber security is now gaining more attention worldwide. According to the SiteLock 2019 Website Security Report, there were an average of 80 cyber-attacks per day worldwide in December 2018, and about 1% of all the websites are infected.

In the days when the railway systems were very much isolated systems operating independently, cyber defence was not on anyone's agenda and none of these systems were equipped even with a simple virus checker or any sort of immunization software.

According to wikipedia.org, there were about 200 CBTC installations worldwide at the end of 2018, many of which are Wi-Fi based using the public accessible 2.4GHz or 5.8GHz band for the communication with trains, and an Ethernet based connection between computers and systems, with a "connect as necessary" internet connection. This signifies there are access paths available for the hackers to penetrate the railway infrastructure, a vulnerability that may impact railway safety.

Moreover, cyber attackers are no longer individual computer geeks working from their bedroom or basement at home, hacking their way to prove their IT skills and capabilities. These groups of "organized digital criminals" are now catching more attention from infrastructure owners: 90% of the key installations in the United Kingdom had been hit by at least one successful cyber-attack. There is no excuse that the railway industry will be exempted from this growing trend.

2.2 Types of Cyber Attacks

There are two broad motives behind a cyber-attack on a particular IT based system: hacking the security at the entry point from an internet, Wi-Fi or radio system access to the system, with intentions to enter the system and gain valuable information stored in the system concerned; or cracking the system from the internet side causing malfunction or system breakdown. In November 2017, the Domestic Security Council and the Cyber Council of the Intelligence and National Security Alliance (INSA) in the USA organized a table top exercise on a cyber-attack of a critical infrastructure (a power company was selected as the target) and the related response and recovery mechanisms. This exercise helped the INSA and its members discover the vulnerabilities within the system and what improvement measures on detection, response and situational awareness needed to be implemented. This simply implied the services provided by this critical infrastructure could cease if a real cyber-attack was to take place.

Figure 1: INSA table top exercise 2017-11-08 [CREDIT: INSA]

Before we understand how one can protect the railway infrastructure from cyber-attacks, we should know what these threats are and how they manage to penetrate into our system. Not all of the threats are applicable to railway infrastructure but knowing their operational mechanism will help us design appropriately preventing future attacks. We will discuss a few of the cyber threats that are more relevant to railway systems.

2.2.1 Wi-Fi Access

About 10 years ago, in the early days of Wi-Fi based CBTC system, there had been reported cases of hackers attempting to intrude into signalling systems from Wi-Fi Access Points from metro station platforms. Over-the-air communication is always a difficulty to protect from unauthorized access as Wi-Fi access hacks are the most common cyber-attacks. It can be broadly categorized into three different types: Man-in-the-Middle (MitM) attack, Wi-Fi security breach and unknown or rogue access point.

MitM attacks are commonly found in public or free Wi-Fi systems where a hacker sets up a router pretending to be the public Wi-Fi service in the area. The usual mode is to set up a Wi-Fi repeater or a router with a similar name to the public Wi-Fi service. Once the client device is connected to the fake router, all the data traffic in and out of the device is captured. In addition, the hacker may install malicious software onto the client device giving him all the data traffic from this device from this point on even after the device is disconnected from the fake Wi-Fi service. The MitM attack is quite difficult to trace in the internet world.

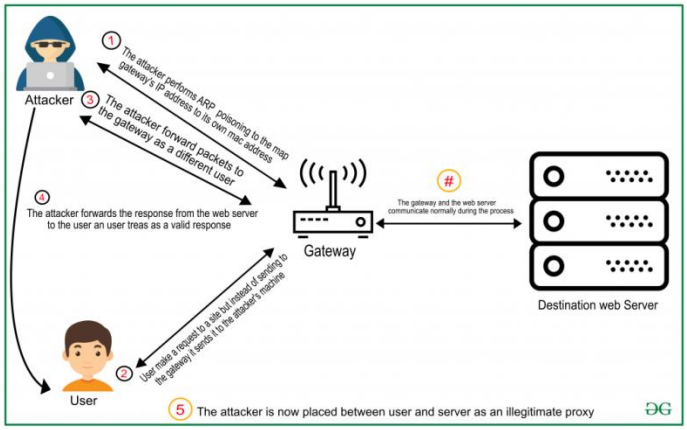

Figure 2: MitM Attack [CREDIT: GeeksforGeeks]

When I want to connect to the IRSE website from Hong Kong, this is in the internet world a direct connection, as many would perceive. I did a trace of the connection from my laptop and found that the connection was routed from my laptop to the Wi-Fi router, the ISP router, 3 more locations in Hong Kong, and 5 intermediate hops in London (between 2 ISP companies) before reaching the destination. A total of 11 servers or routers in between. This means that inserting one more intermediate step would be very difficult to spot.

```
Tracing route to www.irse.org [130.193.90.234]
  1     2 ms     1 ms     1 ms  192.168.46.1
  2     *        *        *     Request timed out.
  3    78 ms     5 ms     3 ms  10.12.5.41
  4     4 ms     3 ms     4 ms  tswc9242.netvigator.com [203.198.19.242]
  5   324 ms   306 ms   306 ms  63-218-231-41.static.pccwglobal.net [63.218.231.41]
  6   260 ms   270 ms   244 ms  TenGE0-4-1-0.br01.ldn04.pccwbtn.net [63.218.242.41]
  7   328 ms   304 ms   307 ms  ten0-1-1-2-t40-mse1.router.uk.clara.net [195.66.224.66]
  8   327 ms   307 ms   306 ms  tengige0-0-1-2-gs2-ar6.router.uk.clara.net [195.157.252.3]
  9   327 ms   307 ms   239 ms  be2-gs2-mse1.router.uk.clara.net [195.157.3.22]
 10   252 ms   278 ms   306 ms  po1.br1.str.uk.idllt.net [80.168.71.254]
 11   328 ms   306 ms   244 ms  gi5-2.ir3.str.idllt.net [78.40.33.30]
 12   329 ms   242 ms   371 ms  xvm50534.vps.cloud.tagadab.com [130.193.90.234]
Trace complete.
```

Figure 3: Trace Log file

A Wi-Fi security breach quite often occurs at home Wi-Fi routers, where people just forget to setup password protection or uses the simplest security of Wired Equivalent Privacy (WEP). According to ABC news in the Houston, TX, a mother learnt that her daughter's bedroom CCTV camera was hacked into from an online game.

There are also numerous stories about third party using someone else's Wi-Fi as it was not password protected. There are also many, many cases of user name: admin, password: password Wi-Fi routers that give wide open access to anybody, period.

With the abundance and relatively low cost of IT hardware with open source software available, it is extremely easy for any person to setup a Wi-Fi access point hence hackers can gain access to your data and even manipulate your actions. A rogue access point is a wireless device installed in a certain network without the authorization or knowledge of the network administrator. It can be connected to the network through a LAN port on the router, a wall LAN port connector, USB device, or even hidden inside the server or client PC. According to Gary Glover of SecurityMetrics, these devices are connected inside the internet firewall hence are lethal to security breach. These hackers install such devices inside the network, with ease, using a technique called social engineering, allowing them to convincingly work their way through the premises. Such techniques have been presented in the 2002 DiCaprio and Hank movie: "Catch Me if You Can", which was based on the true story of Frank Abagnale. In real life (and in the movie), Abagnale used multiple false identities and successfully deceived airlines, hospitals, banks, and even the Attorney General's office of Louisiana. Similarly, after successful entry physically into the target's premises, these social hackers would be able to setup the equipment to "*hack from within*" that any security detection system guarding the firewall would be rendered useless!

2.2.2 Ransomware, Malware and Malicious Attachments

Ransomware, malware and many other types of similar "hidden software" packages disguised in many forms have been one of the most common form of intrusion to a secured network. According to Geraldine Strawbridge of MetaCompliance, the WannaCry attack in 2017 affected 200,000 victims in 150 countries.

Figure 5: Ransomware Hijacks SF MUNI [CREDIT: mount-tech.blogspot.com]

Figure 4: WannaCry at a German PID [CREDIT: @ZEICHENTATEN/TWITTER]

Malware is designed to damage devices, steal information or cause mayhem to the target computer system or network. Malware can be broadly categorized into:

- *Virus*, which is attached to clean executable files with an intent to damage core functionality of the system, and removing / corrupting useful information;
- *Trojan*, which is used to create backdoors in the security to let the hackers enter the target network;
- *Spyware*, which hides in the background and collects the user's valuable information such as passwords, financial data, or anything that may be of value to the hacker;
- *Worms*, which is a piece of software infecting sequentially the devices on the target network;
- *Ransomware,* which is designed to lockout the legitimate user from accessing their information until a ransom is paid;
- *Adware,* which displays advertisements to the user. Although it does not damage the system, but is rather annoying;
- *Botnet*, which are infected computers (known as zombies) on the same network which are now under the control of the hacker. These zombies are then used in a coordinated manner to launch major mayhem to other networks.

2.2.3 Removable Media and USB

In November 2018, researchers at Honeywell International Inc. released the *Honeywell Industrial USB Threat Report* describing the increasing trend of an industrial control system's security being breached by the USB removable media. At their Secure Media Exchange centres at 50 locations around 4 continents, they found an incredible 44% of these locations detected and blocked at least one malicious file that may have a security issue associated. The report validates that the threat of computer security is no longer only applicable to commercial systems, but all systems concerned. This is indeed a wakeup call to industrial control security experts who thought their systems were of little value to the hackers.

USB removable device attacks are somehow very difficult to detect due to the small size, ease of concealment and ubiquity.

Figure 6: A small USB drive with a 5 cents coin [CREDIT: SanDisk.com]

Researchers at Ben Gurion University of the Negev in Israel complied the various types of USB related cyber-attacks and grouped them into four categories:

- reprogrammable microcontroller attacks;
- maliciously reprogrammed USB peripheral firmware attacks;
- attacks based on unprogrammed USB devices; and
- electrical attacks caused by USB killers, which permanently destroy equipment when a USB triggers a rapid electrical charge/discharge cycle.

Another interesting fact from tests by the researchers is that people picked up suspicious USB media left on the street or at a café table and inserted it into their computer without hesitation, just curiously wanting to find out what is stored on it. Another research showed that USB media is often the culprit of "jumping the air gap" infecting the otherwise completely isolated network computers.

2.2.4 Denial of Service

A Denial of Service (DoS) attack is one where a hacker attempts to prevent legitimate users from accessing the target system's services. The usual mode of operation of these DoS attacks is that the hacker sends authentication requests to the server which have invalid return IP addresses. A DoS attack can be executed in one of the following manners:

- Flooding the network to prevent legitimate network traffic;
- Disrupting the connections between two machines, thus preventing access to a service;
- Preventing a particular individual from accessing a service;
- Disrupting a service to a specific system or individual; or
- Disrupting the state of information, such resetting of TCP sessions.

The main objective is to cause excessive network traffic in and out of the server, causing the server CPU to run extensively processing these junk requests preventing the normal tasks from being performed.

A Distributed Denial of Service (DDoS) attack builds on the DoS principles but employs multiple IP addresses to coordinate such an attack.

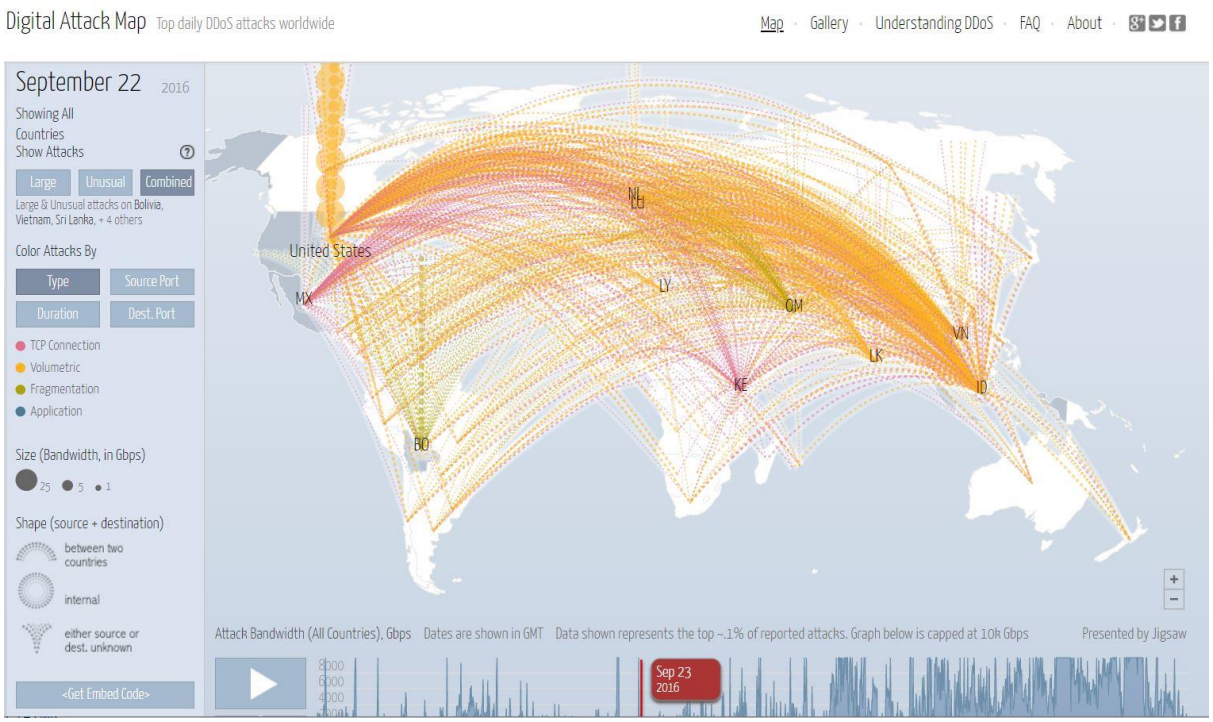

Figure 7: DDoS Map as at 2016-09-22 [CREDIT: DigitalAttackMap.com]

For signal engineers and railway operators, one would consider DDoS attack is something of a lesser concern, as their signalling system is "physically disconnected from the internet". With the wide adoption of Wi-Fi based train to track communications for the modern CBTC systems, the breach may come from the Wi-Fi Access Points again.

3 HACKERS AND THEIR AMBITION

Hackers break into computer networks in order to steal, change, or remove information that would be of value either to themselves or the legitimate users. The most famous one being the WannaCry ransomware attack in 2017 when over 200,000 fell victim to these hackers. Railways are no exception as I have pointed out in Paragraph 2.2.2 above. In some other cases, the hackers would want to make a statement, or to seek a political cause. For example, by breaking into an enemy state's national defence network can damage their capabilities of mobilizing the military strength; or breaking into a power grid in order to cripple a city's normal function.

Unfortunately, railway falls into the above categories: (1) it can slow down mobility of citizens and armies; (2) it can cripple a city's function; and (3) it is of high value to the owners. So far we have seen many occurrences of cyber-attacks on railway around the world, and the trend is growing. Examples are attacks on Great Western Railway and Deutsche Bahn in 2017 and the Danish Railway in 2018.

4 CYBER SECURITY FRAMEWORK

The National Institute of Standards and Technology published on 16 April 2018 version 1.1 of the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework, or CSF). This framework was first developed (version 1.0) under the USA Executive Order 13636 that "*Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats*".

The CSF employs a risk mitigation based approach, similar to the system assurance process we railway engineers are now very familiar with. The CSF is made up of three principal elements:

- **Framework Core** is the set of activities, expected outcomes and references on all the aspects and methods on cybersecurity;
- **Implementation Tiers** are the actual implementation of managing vulnerabilities and possible threats; and
- **Framework Profile** is the set of organization parameters and requirements on cybersecurity and the level of cybersecurity risk they would be able to take.

The Framework Core is defined as a matrix of functions and categories:

Function	Categories
Identify	• asset management • business environment • governance • risk assessment • risk management strategy
Protect	• access control • awareness and training • data security • data protection processes • maintenance • protective technologies
Detect	• anomalies and events • continuous monitoring • detection processes
Respond	• response planning • communications • analysis • mitigation • improvements
Recover	• recovery planning • improvements • communications

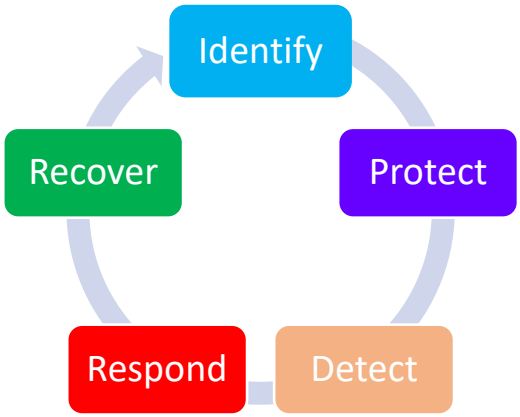

Figure 8: NIST CSF Core

The BSI Group recommends a seven step approach to the implementation of the CSF:

Figure 9: Seven Step Approach to CSF

In fact, when we look at systems assurance, quality assurance and the cybersecurity framework, there is a lot of similarities between them, this would be a benefit to the railway organizations as their staff are very conversant with the former two.

5 MANAGEMENT APPROACH TO CYBER SECURITY RISKS

The protection of a CBTC system from hackers must be addressed from the top to bottom of the organization, as well as requiring the full commitment from all personnel. The ISO 27000 series of standards on best practice for an Information Security Management System (ISMS) and NIST CSF require the practicing company to implement a risk based approach to infrastructure management for managing information security. ISO 27004 requires the development of an impact-likelihood matrix for the concerned cybersecurity risks, and the system / procedure must fully address the high and medium risk items and look at the low risk items on a cost effectiveness basis: very similar to the ALARP principles we all are familiar with.

According to Schlehuber, Tews and Katzenbeisser, there is a VDE draft standard for IT security in railway signalling applications being reviewed (DIN VDE V 0831-104). This standard is based on IEC 62443 and is compatible with EN 50129. At the moment signalling suppliers have developed their own versions of cybersecurity for their CBTC systems based on their understanding to NIST CSF, ISO 27k, or IEC 62443. This again has a very close resemblance of the early days of CBTC when each supplier went on a slightly different path of implementation [Bechtel (on specifications only), Siemens, Thales].

6 SYSTEM DESIGN FOR CYBER SECURITY

Upon the submission of the Fennel and Hidden Reports on the two major railway accidents in the 1980's system safety by design has become a norm in railway engineering, especially in railway signalling design where major improvements have been made in a systematic and structured approach to signalling system implementations around the world.

Now the signalling world has moved to the level in the cyber space, signal engineers now must take a proactive role to ensure the signalling system designs are up to the challenge we face in the IT world. We must not be seen as reactive as we did 30 years ago, especially that we already have GoA 4 trains where we rely fully on the automated systems.

About 10 to 15 years ago, we were still very comfortable to declare that the signalling system is self-contained, completely isolated from the internet where hackers are always around the corner. With CBTC systems, connections to the communications facilities including (1) radio; (2) CCTV; (3) PDIS, (4) PA, and many others, the signalling system is no longer immune from any of the cyber threats. Furthermore, the system software is upgraded from portable media making the system upgrade vulnerable to cyber-attacks.

Once malware is planted via a USB media device onto a system server, the Trojan code can execute malicious software from within the firewall, and can utilize the Wi-Fi CBTC connection to connect to hackers from the outside.

This implies that we should not solely rely on ring fencing the system preventing external access, but also threats from within. Unfortunately, CBTC systems are not yet designed to protect themselves from such weaknesses.

In most signalling system specifications, we now have a specific section of system safety where we prescribe the system safety requirement, safety assurance activities and the system safety targets for the railway concerned. A similar set of requirement for cyber security should now be a norm for the new CBTC systems moving forward.

With end users and suppliers subscribe to these common requirements, or even incorporated into the CBTC standards, the IT security of signalling systems can be enhanced. This set of requirements should contain, as a minimum:

- compliance to NIST CSF, ISO 27k or IEC 62443. I believe we should come up setup a working group to formulate the minimum framework requirement that industry suppliers can comply with, the railway operators are comfortable with and a future migration and upgrade capability: Autonomous trains are not far away from reality and cyber security for these trains must be considered a core design requirement.;
- a set of cyber security targets and parameters including such parameter of cyber critical failure rate (mimicking that of the SIL) and failure impact and extent. For example, a cyber-attack on a Wi-Fi access point may only affect the communication to that single access point only. This allows the system to be designed with redundant channels in a hot standby configuration;
- limited ports and restricted access from the internet and interfacing systems. This will ensure the infection is controlled and contained;
- appropriate system upgrade procedures eliminating the possibility of unwarranted third party software becoming embedded in the CBTC system;
- highest level of access control protocol for the human machine interface of the CBTC;
- building in cyber threat detection mechanisms to alert operators of potential intrusions; and
- restriction on the use of open source software, to prevent hidden backdoors being planted.

I believe the IRSE should champion a work group with the concerned stakeholders drafting a guideline on more comprehensive cyber security requirement for railway signalling systems.

7 OPERATIONS REQUIREMENTS AND HUMAN BEHAVIOUR

While we endeavour to make the CBTC system cyber secure, it is also important that operators and maintainers behave appropriately as well. As I pointed out in Chapter 2 above, much of the malicious software is brought into the system through carelessness of the personnel, inserting an infected USB media device to the servers or workstations.

I have encountered many companies, especially information technology and security related ones, that restrict the use of these portable devices at work. These devices are only allowed at a certain location where appropriate defence software is running. This is now a common practise for many end users to enable those ports that are absolutely necessary for operations purposes.

Furthermore, NIST CSF requires a management framework be in place to ensure compliance and adherence to the framework at all times. Regular cyber security audits, similar to quality audits or system safety audits, must be conducted and the cyber risk threats matrix should be updated periodically as well. What is needed is a Cyber Security Policy and operations procedure to be developed, prior to the commencement of passenger service. Cyber security should also be a mandatory item on the management meetings, similar to quality, health & safety, and environmental protection.

8 ON THE HORIZON

The 21st century is commonly known as the information age and railway signalling is moving forward to meet this new age as well. We are now not too far away from autonomous vehicles and I can see autonomous trains to be not far behind. We must ensure our CBTC system designs are future proof so that we do not need to start from zero again for the future.

Furthermore, the Internet of Things (IoT) is entering into the mainstream and 5G mobile networks are two to three years down the road, these may bring additional challenges to the CBTC system design.

9 CONCLUSION

For the past thirty years, railway signal engineers have advanced immensely in the concept and development of system safety. For the next generation, the focus will shift to cyber security. Whilst system safety related issues do not change too much, cyber security is a completely different beast, with new threats coming out by the minute. CBTC designs must address the cyber security risks today and be ready for new hazards tomorrow. Our mind-set must adapt to the new world order in order to provide a safe and secure train service to our passengers.

10 REFERENCES

1. Hirsch R., Editor. *Managing Railway Operations and Maintenance: Best Practices from KCRC*. London: A & N Harris and University of Birmingham Press, 2007.
2. *How many phones are in the world? [online]* https://www.bankmycell.com/blog/how-many-phones-are-in-the-world [2019-05-20]
3. *What is Cyber Security*. [online] http://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html [2019-04-10]
4. *CyberSecurity Statistics for 2019*. [online] http://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/ [2019-04-10]
5. *Cyber Attacks Increase by 59%, Is Your Small Business Safe?* [online] http://smallbiztrends.com/2019/05/2019-cybersecurity-statistics.html [2019-05-30]
6. Communications-based train control. [online] http://en.wikipedia.org/wiki/Communications-based_train_control [2019-03-23]
7. *Cyber-attacks 'damage' national infrastructure*. [online] http://www.bbc.com/news/technology-47812479 [2019-04-05]
8. *Wireless Access Point Protection: Finding Rogue Wi-Fi Networks*. [online] https://www.securitymetrics.com/blog/wireless-access-point-protection-finding-rogue-wi-fi-networks [2019-05-15]
9. *WAKE UP CALL: Mom learns daughters' bedroom webcam was hacked*. [online] https://abc13.com/news/mom-learns-daughters-bedroom-webcam-was-hacked/1465134/ [2016-08-11]
10. *The Dangers of Ransomware*. [online] https://www.metacompliance.com/blog/dangers-of-ransomware/ [2019-02-25]
11. *Honeywell Industrial USB Threat Report.* Houston, TX: Honeywell Process Solutions, 2018.
12. *USB attacks: Big threats to ICS from small devices*. [online] https://searchsecurity.techtarget.com/feature/USB-attacks-Big-threats-to-ICS-from-small-devices [2019-02-08]
13. Howe N. *Cybersecurity in railway signalling systems*. IRSE News Issue 236, 2017.
14. *CYRail Recommendations on cybersecurity of rail signalling and communication systems*. CYRail Consortium, 2018.
15. *Managing a Cyber Attack on Critical Infrastructure: Challenges of Federal, State, Local and Private Sector Collaboration*. Arlington, VA: Intelligence and National Security Alliance, 2018.
16. *Framework for Improving Critical Infrastructure Cybersecurity, version 1.1*. Gaithersburg, MD: National Institute of Standards and Technology, 2018
17. *The Framework for Cybersecurity – Who Needs It and Why? – A White Paper*. London: BSI Group, 2015
18. Sigurdsson R. *The 2019 Essential Cyber Security Threat List*. Reykjavik: AwareGO, 2019.

19. Pong R. *Practical Implementation of ISO/IEC 27001 in Your Environment*. Hong Kong: Hong Kong Council for Testing and Certification, 2018.
20. Phinney T. IEC 62443: *Industrial Network and System Security*. Durham, NC: International Society of Automation, 2011.
21. Rogers D. *IEC 62443 A cybersecurity standard approaching the Rail IoT*. Vienna: Intelligent Rail Summit and Siemens AG, 2017.
22. Schlehuber C., Tews E., Katzenbeisser S. *IT-Security in Railway Signalling Systems.* Darmstadt: Technische Universität Darmstadt, 2014.
23. *Cybersecurity for Public Transportation Rail Systems – The Bechtel Approach*. Gaithersburg, MD: National Institute of Standards and Technology, 2018.
24. Kispert C., Ruedebusch T. *Cybersecurity For Rail: Not A Single-Shot Approach – Applying the NIST approach to rail transportation*. Vélizy-Villacoublay: Thales Ground Transportation, 2016.
25. Hidden A., QC *Investigation into the Clapham Junction Railway Accident*. London: Her Majesty's Stationery Office, 1989.
26. Fennel D., QC *Investigation into the King's Cross Underground Fire*. London: Her Majesty's Stationery Office, 1988.
27. *Cybersecurity Insiders - Cyber Attack on Great Western Railways,* [online] https://www.cybersecurity-insiders.com/cyber-attack-on-great-western-railways/
28. *The Local – Cyber attack hits Danish rail network,* [online] https://www.thelocal.dk/20180514/cyber-attack-hits-danish-rail-network