The Institution of Railway Signal Engineers Inc

Australasian Section Incorporated

Rail Telecommunications – The Coming of the Digital Age

Nick Czeperko
Independent Consultant

Blair Zanon
Independent Consultant

Jacek Mocki
CPEng MIRSE NPER
MOTZKY

SUMMARY

Railways were conceived as part of the 1st industrial revolution, as steam & water power started to transform the way society at the time manufactured, interacted and consumed. Following this the other industrial revolutions have followed – mass production using electric power, which also included the rapid development of the railways and digital automation. The next revolution often referred to as big data or Internet of Things (IoT), is now well on the way.

Telecommunication to control today's railways dates back to a pre-digital age, increasingly, becoming less efficient than the modern options. Advancements are now in use around the world that can make maximum use of the space available without compromising safety. Change is coming – whether we are ready for it or not! The arrival of the "information everywhere world" (a world where sensors continually transmit data, ready to be interpreted, analysed and processed) has opened up some new opportunities to make existing technology in the rail network more efficient and reliable using intelligent network solutions.

The Australian Railway network retains a significant aspect of the second industrial revolution. Diesel fleets currently in use are not much different in principle from their predecessors. Until recently token-based signalling systems were in use on main line railways. Relay-based signalling systems are still relevant in Australia. Third revolution interlocking (using digital technology such as programmable logic controllers exist, but are not yet common place.

Each state has their own requirements for infrastructure and rolling stock. This fragments supply and increases costs for bespoke solutions and low production runs, hence the barrier for replacement and upgrade is high.

This paper highlights how Digital Connectivity in Rail can provide detail information for better decision making and empower the travelling passengers before, during and after their travel.

Digital Connectivity will and in some instances already is delivering information to the people who are qualified to make informed decisions. The collection of big data will be transformative, allowing the operator to predict and avert equipment failure, hence reducing the prospect of delays across the network. The overall outcome of mapping assets will allow maintenance teams to find and locate equipment much easier than previously possible.

Networked infrastructure and analytics has the capacity to make this happen.

1 INTRODUCTION

What is Digital Connectivity? – It is defined as "*the function of devices transferring data back and forth, with the aid of bridges, hubs, switches, routers, along wireless, copper and fibre backbone networks*".

Conventional signalling and train control systems (currently in use), in some cases reduce the potential capacity and flexibility of the telecommunication network, which struggles to recover quickly when things go wrong.

Railways are divided up into signalling sections known as "blocks". The signalling system keeps the trains safe by only allowing a train to enter the "block", once the previous train has cleared it.

While this maintains a safe distance between trains, however it makes inefficient use of the railway infrastructure. This inefficiency isn't a problem if there are plenty of spare blocks between trains so they can keep moving on a wave of green lights, but once the railway fills up, trains must move in lock-step as they wait for blocks to be vacated; a small delay to one train can cause massive knock-on effects.

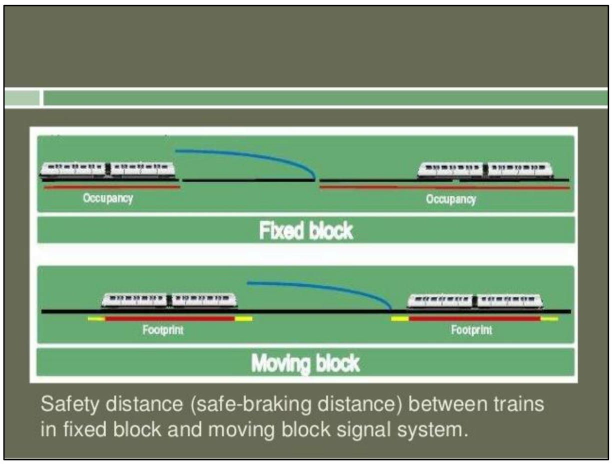
Even a single disruption can cause a chain-reaction of delays. For example:

During the construction of the Moreton Bay Rail link project in Brisbane, the Queensland Government was informed of serious signalling problems which caused a delay opening of the rail network.

"*The rail signals are the traffic light system of the network"* said Mr. Hinchcliffe – Qld Transport Minister.

Mr. Hinchcliffe was further quoted saying, under the current system three trains could not pass through the Petrie Station, without the system crashing. The system should be able to handle 26 signalling changes at once when the train pass through the station, but was failing after 15. [1]

By upgrading telecommunication networks in signalling and traffic management (allowing digital connectivity), introduces a command and control system that creates a safety buffer zone around trains, which is informed by trains communicating their position in real-time, where the buffer zone moves with each train effectively forming a ‘moving block’ safety envelope around it



Safety distance (safe-braking distance) between trains in fixed block and moving block signal system.

Figure 1 – Buffer Zones around trains

The adoption of digital connectivity enables operators to deliver even safer services and more efficiently, to use live data reducing delays due to signalling errors and to make the telecommunication systems more available.

1.1 LITERATURE REVIEW

Digital connectivity, big data, internet of things and cyber-security are evident in the literature.

A survey of existing wireless techniques used in the railway industry for both communications and signalling purposes is widely discussed in [2]. Authors are focused on finding a low-cost and low-power wireless sensor networking techniques to monitor the conditions of railway wagons.

Roadmap for digital railways [3] provides some framework on formalising digital connectivity, safe voice communication and cyber-security.

Deloitte’s report [4] highlights the beginning of a digital era where the technology has brought us smart phones, real-time planning, open traffic data and social customer service. For the first time, the passenger now has more information than the operator.

The authors of “Strategic Rail Research and Innovation Agenda” [5] discuss the future of rail transport. They emphasize customers are the future of rail transport. To be successful the rail transport needs to continue growth in the following areas: Capacity, User, Safe and secure, Technological breakthrough and competitiveness of the rail sector, Optimised design and operation/connectivity/interoperability, Maximised value for money leading to modal shift, Efficient & environmentally sustainable, Reliable & resilient skills.

The white paper [6] serves as a guideline for 5G definition and design, and provides also insight into areas of further exploration by NGMN (a body established to develop 5G technology) and other industry stakeholders. In rail sector, we just started using 3G technology for our digital connectivity. The technology is developing extremely fast.

In the “Robust Railway Operations” talk [7], Professor David Pisinger presents a lot of interesting information on sources of big data in railways; he highlights disruptions and gives some examples of how big data is applied for robust rail operations.

Another article worth reading on big data is produced by the Parliamentary Office of Science & Technology in the UK. The transport sector has always collected and analysed large quantities of data, such as data from timetables, traffic news and air schedules. However, recent developments in the quantity, complexity and availability of data collected from and about transport, together with advances in computing technology, are presenting new opportunities to create more efficient and smarter transport systems for people and freight. [8]

Publication [9] is an example of how we could analyse the data. Authors use mobile geolocation data and public transit data for generating complete insights on public transit travel patterns. They applied trajectory analytics on mobile geolocation data and showed that the limitations of mobile geolocation data can be addressed by leveraging the complementary strengths of public transit data via appropriate calibration and learning. Authors have shown that combining these data sources helps provide an accurate and complete picture of public transit trips, including first and last mile.

Also, Peter Hughes in [10] tries to use big data to risk analysis that can work to the advantage of railways in the UK. He provides some practical examples on how to build enterprise architecture for data to work for railways.

Oracle in [11] guides us to big data. This position is a great explanation what the database is, how to organise the data, how to secure the data, how to visualise and analyse the data.

Finally, some interesting and honest view on the Industrial Internet of Things is presented by World Economic Forum in. [12] For example, authors have conducted a survey. The question was: What are the greatest barriers inhibiting business from adopting the industrial Internet? Not surprisingly, almost two-thirds of respondents agreed with the widely-held view that security and interoperability are the two biggest hurdles. Other significant barriers cited include the lack of clearly defined return on investment (ROI) (53%), legacy equipment (38%) and technology immaturity (24%).

2 RAIL BACKGROUND

Currently, there seems to be a desire to introduce a new type, or types of signalling system on the rail market in Australia. Rail infrastructure owners think about an introduction of Communication Based Train Control system (CBTC) and European Train Control System (ETCS) level 2 and 3, where wireless communication replaces a standard cable communication. Australia, in some literatures defines those systems as “non-conventional” signalling systems as opposed to the conventional systems currently in use such as mechanical, or electro-mechanical interlocking, relay interlocking and computer based interlocking that are controlling colour light signals and point machines on the railway track in the response to the occupancy of track sections.

When CBTC is applied, trackside and track circuits are not used. Position is determined by a two-way communication between the train and wayside. Train transmits position, while wayside transmits a target point. The train's position can be transmitted within a centimetre. To what extent can we trust things, such as intelligent industrial networked devices? Will they behave as expected, or will they be interfering with unlimited Internet access? To what extent can we manage and control the telecommunication devices? Will our lives become unpredictable and uncontrollable with widespread use of the Industrial Internet of Things (IIoT)?

Engineers generally assume that mechanisms serve their intended purpose. Is that always true? The "smarter" a device is, the quicker we lose control and become fully dependent on it. As smart devices demand greater attention, will they demand ongoing fine control and management?

As an example, the rail control centre is a very complex organisation that houses all signalling signallers and operators. The systems that have been used to control and communicate are located along the routes in huts, stations, road crossings, signal towers, tunnels, maintenance yards, power stations, refuelling depots, local control rooms and operations control rooms. There are also key parts of the control system buried under, or alongside the rail lines and signals that are transmitted in the rails, or via specialised aerial paths.

The rail control centre needs to combine dozens of systems, including some but not limited to the following, which all have the capacity to utilize the benefits of digital connectivity:

- access control systems advertising
- closed-circuit television (CCTV)
- control and communication
- emergency communications
- grade crossings
- passenger information systems
- people-moving systems
- signals and train control
- ticketing systems
- vital communication-based train control (CBTC), automatic train protection (ATP) and signalling.

In the past, many of these systems were analogue or mechanical devices, hence did not have any need, or method to communicate with each other. The connections between and among them were usually direct connections such that one wire connected to another device without any sharing communications-except the cable that the wire was enclosed in.

Today's environment has changed, so that the communication between and among devices is digital via Ethernet, Transmission Control Protocol/Internet Protocol (TCP/IP) or a similar networking standard. This standardisation gives new capabilities.

Before we get into greater discussion, it is extremely critical to introduce and define few main areas of interest.

3 DEFINITIONS

DIGITAL CONNECTIVITY is defined as "*the function of devices transferring data back and forth, with the aid of bridges, hubs, switches, routers, along wireless, copper and fibre backbone networks*".

Simply describing the outcome, more trains on tracks, providing a safer, secure, more reliable network system for both the customer and the operator.

The Internet of Things (IoT) is one of the areas in digital connectivity, when implemented, will enable further automation of train operations which will increase the efficiency, punctuality, capacity and performance of the railways.

BIG DATA, - the term 'Big Data" has been around since the 1990s and is defined as the volume of information that inundates all businesses, including the rail network on a day – day basis.

It also refers to the use of predictive analyses by extracting value from the data being generated.

"It's important to remember that the primary value from big data comes not from the data in its raw form, but from the processing and analysis of it and the insights, products, and services that emerge from analysis. The sweeping changes in big data technologies and management approaches need to be accompanied by similarly dramatic shifts in how data supports decisions and product/service innovation." [13]

CYBER SECURITY is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization.

For the rail industry, any cyber system that is used to operate the railway particularly where safety and/or reliability is of importance.

Cyber technology is complex and rapidly evolving, cyber-attacks are becoming increasingly automated and sophisticated.

Railway systems are becoming vulnerable to cyber-attack due to the move away from bespoke stand-alone systems to open-platform, standardised equipment built using "*Commercial Off The Shelf*" (COTS) components, and increasing use of networked control and automation systems that can be accessed remotely via public and private networks. [14]

4 DIGITAL CONNECTIVITY

Digitalization is defined as the existence of information in the form of a code. It relates to the use of code-based software, putting in motion, accelerating, or slowing down certain objects, spaces and processes, which constitute urban life.

4.1 Introduction

Digitalization has been increasingly, even if by default, associated with Internet access and being on-line, although in this particular case a more precise term would be “connection” or “connectivity”, which creates a new type of relationship — almost permanent (ideally and in plans) availability of people and objects.

The arrival of the ‘IIoT” (Industrial Internet of Things) enabling sensors to transfer data, virtually creating a mesh in rail network of “information available technology everywhere”. This has opened new opportunities to make the existing transportation network more efficient and responsive to user demands.

Enhancing operational efficiency goals can include: reducing maintenance, avoiding service interruptions, and improving flexibility to handle varying challenges. Again, new technology is the key to achieving these goals. Condition-based monitoring systems can provide detailed status information for equipment, allowing maintenance teams to perform preventive maintenance that reduces service interruptions. With new communication and signalling systems, intervals between trains can be safely reduced to increase capacity and make more efficient use of the existing infrastructure.

The rail control system needs information to be available, so that trains can be stopped, or started and that boom gates go up and down appropriately. In the area of constrained dollar, the need of accurate and fast information is also critical when dealing in asset management.

4.2 Available Technology

Digital connectivity is supported by mobile and stationery technologies.

Railway operators have achieved the network performance and flexibility they need by combining Ethernet Train Backbones (ETB) with Ethernet Consist Networks (ECN). The complete train control network must be able to manage traffic within inter-carriage and inter-consists while, avoiding IP address conflicts, as well as deliver data from the on-board network to trackside control centres.

Another useful technology to use on the communications layer is wireless bridges for inter-consist data communication. Going wireless for inter-consist communications presents many obvious advantages for inter-train networks

Digital Connectivity, such as Wi-Fi, 3G/4G cellular connectivity can manage the monitoring of: precise position of the train, speed of the train, hence increasing overall capacity.

A NMS (Network Management Software) is important for managing and monitoring network devices. A train’s communication network will include Ethernet switches, terminal servers, and other network devices such as interlocking controllers.

Figure 2 – Trouble shoot Networks with Software Management Tools

Railway operators expect the following features:

- A more visualized user interface that displays physical or pseudo links and Power over Ethernet (PoE)
- Automatic topology discovery
- Real-time link status & traffic statistics
- Real-time alarms via Simple Network Management Protocol - (SNMP) Trap or SNMP Arranges & organises information about devices on the network
- Displays a diverse range of devices used on railway networks (through MIB (Management Information Base) compiler) Visualized Virtual Local Area Network (VLAN).

Figure 3 – Simplify Operations and Maintenance using Network Management Software

4.3 Availability vs Integrity

In any rail operations, network redundancy is a critical factor in ensuring passenger safety, journey reliability in on-board railway communications for both intra-consist and inter-consist Ethernet networks.

In addition, railway operators are looking for ways to more efficiently allocate resources and serve passenger demands. Moreover, the ability to quickly and reliably preserve and reconfigure network settings when consists are rearranged mid-journey is another key factor affecting operational efficiency, passenger safety, and the provision of seamless on-board services and amenities.

The usual Data Communication Systems (DCS) architecture for railway applications is an integrated Ethernet-IP network that includes a wired backbone network, wireless wayside network, and on-board network, with the on-board network handling communications between all communication-based train control (CBTC) sub-systems. A CBTC must be protected by a robust security system, and requires continuous communication in circumstances where roaming is an unavoidable reality and occurs at very high speeds. Perhaps the most crucial aspect of on-board vehicle stations is that they cannot lose any data during handover. For train-to-ground communication links that do not use an improved 802.11 roaming mechanism, the handover time may take up to several seconds. This is not acceptable, particularly since a moving train is only connected to a wayside Access Point (AP) for a few seconds, and handover times that exceed 100ms could result in significant data loss. Reducing this roaming “break time” to a negligible level is a challenge faced by the rail industry. [15]

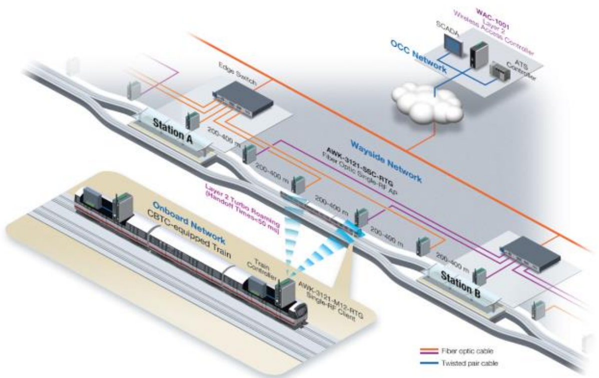


Figure 4 – Minimize Headways with safe operations for CBTC

CBTC uses constant bi-directional radio communications between train & trackside equipment to increase line capacity by reducing headways.

There are cases where integrity is as important as, or more important than availability. For example, it is always important to know where the system’s trains are and that the switches and level crossings are in their correct positions.

Due to recent advances in wireless transmissions, CBTC now heavily rely on WLANs (Wireless Local Area Networks) to ensure constant train-to-ground data connections. The best safeguard in avoiding link failure on a WLAN is through redundancy. This ensures that operations remain “always on” and allows critical network links to continue to transmit data.

Seamless roaming handover with complete redundant Digital Control System (DCS) architecture provides reliable, sustained communication for CBTC operations.

4.4 Digital Disruption

While digital connectivity is a given for new rail networks, it can pose a real challenge to implement in existing networks. As more and more new technologies are offered to the railway market, train operators need to know how to combine them with older systems to enhance operation and service quality. The following section details some key criteria:

4.4.1 IP-based Train backbone options

Two common problems are limited connector pins in the coupler, and limited cables and cabling space in the rolling stock. Leveraging an existing two wire infrastructure to build an IP-based train backbone is a major challenge.

4.4.2 Standard Ethernet:

While IP technology offers great opportunities to enhance your rail service, standard Ethernet requires four wire cable to reach 100 Mbps and eight wire cable to reach 1 Gbps. Cable is almost always a limitation in refurbishment projects, so standard Ethernet may not be the best option.

4.4.3 VDSL (Very high bit rate DSL):

This technology makes it possible to use two wire cable for a high-speed IP-based train communication backbone. However, VDSL has some limitations, such as longer negotiation time for setting up an Ethernet communication link, which could make some applications slow to respond.

4.4.4 Collecting extra signals to monitor train status

In some cases, it is difficult to collect data from the existing train, or legacy devices. You may need to add extra sensors to collect physical signals such as temperature, door status, or HVAC status.

PLC (Power Line Communication):

PLC routes data over the train’s existing power cables to create an IP-based train communication backbone. PLC is a mature technology, as it was originally developed for home automation. PLC can reach about 50 Mbps in industrial applications.

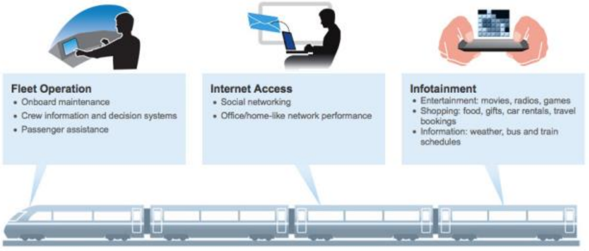

Fleet Operation
• Onboard maintenance
• Crew information and decision systems
• Passenger assistance
Internet Access
• Social networking
• Office/home-like network performance
Infotainment
• Entertainment: movies, radios, games
• Shopping: food, gifts, car rentals, travel bookings
• Information: weather, bus and train schedules

Figure 5 – What can be achieved with an on-board Wi-Fi Network?

4.5 Digital Connectivity – Choice for individual Passengers

Beyond simple Internet access, railway operators have also begun to recognize that they can leverage on-board Wi-Fi networks to support a variety of operational and passenger infotainment applications. A digitally-connected fleet enables real-time system status reporting and better information flow. These services make operations more efficient, reducing costs, improving service quality, and raising customer satisfaction.

New technology helps deliver these goals by enabling useful information services, such as train schedule information, transit information, train location and weather reports. Passenger Wi-Fi and on-board entertainment are also important for passengers throughout their journey.

The huge growth in use of smart phones and Wi-Fi-enabled mobile devices is the catalyst for the increased usage and ubiquity of Wi-Fi connectivity in public places. In response to the explosive growth in data volume, service providers are off-loading traffic from their cellular networks to Wi-Fi networks. Additionally, the changes in user behaviour and data network landscape have created a huge challenge for railway operators to provide enough bandwidth for each passenger in a high-density environment. A traditional enterprise Wi-Fi deployment— just aiming to provide coverage—is no longer enough. In a high-density Wi-Fi infrastructure, operators must look for a solution that combines reliability, coverage, bandwidth capacity, to ensure a seamless user experience. For example:

“Due to the advent of high capacity bandwidth technology, a new approach to map the new age Synchronous Data Hierarchy (SDH) rail networks is needed. The traditional drawing methods employed by rail owners to describe the Plesiochronous Data Hierarchy (PDH) constructed networks, - transportation of large quantities of data over modes such as fibre optic and microwave radio networks - currently in use, is no longer applicable. In a long run, it will create some significant problems to the rail owners as they will have difficulties to model upgrades and connections of new SDH networks.” [16]

In addition to the above, railway operators must implement client isolation in a public Wi-Fi network to prevent client devices from communicating with each other. By considering several important factors – network reliability, data rate, mixed mode client ratios, load balancing, and network security – railway operators can choose an effective Wi-Fi solution that meets the requirements of rolling stock application satisfaction. [17]

This serves two purposes—it increases network security and limits broadcast traffic. Every device that connects to on-board APs (Access Points) belongs to the same network, including on-board systems such as broadcast, or other control systems.

One key solution is wireless client isolation. This prevents wireless clients from directly communicating with other’s wireless devices on the same network. This offers an added layer of protection against passengers gaining access to other devices for malicious purposes.

By using this technology, it limits broadcast traffic between wireless devices, hence passengers can utilize the bandwidth that would otherwise be used for broadcast traffic enhancing overall network performance.

4.6 Industrial Internet of Things

The next big evolution of industrial control systems is the “*Industrial Internet of Things*” (IIoT) - physical devices communicating directly with each other, machine to-machine, without human intervention. Smart elements such as sensors, measuring devices, and actuators embedded in control equipment can exchange data in real time, so they can be monitored, integrated, configured, optimized, and managed.

The Industrial Internet of Things (IIoT) is shaping the way industrial applications are designed and implemented today. This is ushering in a new era of operational efficiency, information transparency, and economic growth. Innovative ideas on how to collect data, how to transform data, and how to use the data to increase efficiency and reduce costs are sprouting up all around us. The IIoT has bridged the gap between the physical and digital worlds and has created one combined space that provides limitless possibilities.

Unfortunately, the IIoT is also a new frontier for potential cyber-attacks.

The sheer scale of the Internet of Things massively complicates familiar security issues. The number of Internet-connected devices is estimated to reach 50 billion by 2020.

5 BIG DATA

“Everything is a big-data problem right now. The biggest change is that every device, every vehicle, everybody is manufacturing huge amounts of information.” [17]

5.1 We have no Big Data – why is it a problem?

The power of Big Data will allow the operators to trace a rash of flat spot problems on wheels to a specific yard and more to appoint, to a specific section of the track, or switch in that yard that is causing the problem. That is the power of big data.

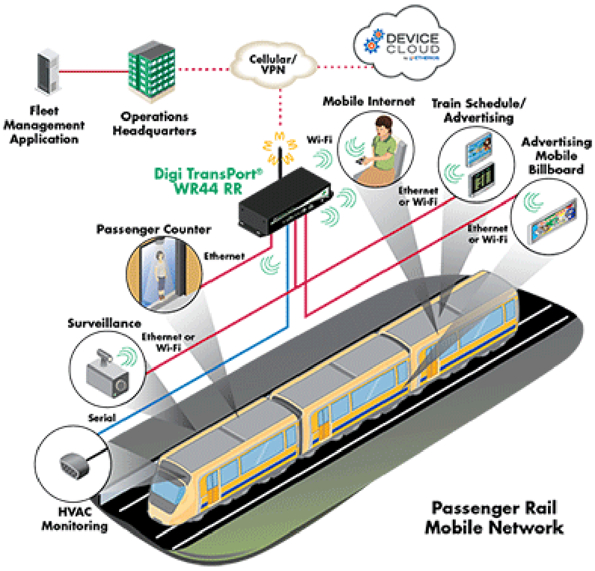


Figure 6 – Passenger Rail Mobile Network

Railways never stop and neither should data. Where the rail industry is, heading is much more than just more of the same data: its more than that, it is real time and it can layer data to increase the intelligence of the information. It allows locomotive fault data to be layered on top of positional data to tell exactly where and when faults occur, the vital signs of locomotives, regardless of external conditions.

One of the applications of maintenance on railways was carried out by Dutch railways on Axle Box Acceleration (ABA) measurements with 1 terabyte of track degradation data for performing adaptive and self-learning mechanisms. Big data was applied in Utrecht, Netherlands to handle the traffic and explain the usage of mobile phones, smart cards and computers to predict the traffic and improve operations accordingly. [18]

5.2 Collection of Big Data

The real “Big Data” challenge is a human one, which is learning to ask the right questions, recognizing patterns, making informed assumptions, and predicting behaviour

We have millions of disparate events and transactions daily, ranging from train movements to customer and employee interactions to smart devices capturing and communicating data.

The Industrial Internet of Things, (IIoT) will bring performance statistics of current rail lines, motors, tracks, systems to the fingertips of every person within the rail industry.

This will allow the entire system to be assessed, the motors, personnel, routes, locomotives, cargo, along with passenger movements are analysed as a network that creates further advances. The inevitable creation of high speed freight trains running at top speeds of 400km/hr on optimized, perfect rail systems. Though eventually everything wears out if the tracks and railways are used to maximum efficiency, however what replaces will be smarter, stronger, and faster.

5.3 Mapping Assets

Traditionally, companies have maintained their business assets using manual processes that are time-consuming and resource-intensive. The IIoT brings with it a complete paradigm shift with respect to the operation and maintenance of industrial equipment. Instead of waiting for equipment to fail before fixing it, or scheduling time-based maintenance that sometimes leads to unnecessary maintenance of equipment and downtime, companies are adopting predictive maintenance strategies to stay ahead of the game. As an example;

A major rail maintenance firm collected data from sensors on its locomotives about the wear of individual components, but personnel still relied on their instincts to determine when parts needed work. The company deployed a solution to sharpen its predictive capabilities and optimize maintenance intervals. Sophisticated software analyses data from on-board sensors along with historical data about components from their asset management system to accurately determine an optimal maintenance schedule. Using data such as date of manufacture, periods of use, places of use and mileage in conjunction with sensor data, the solution calculates cost-effective maintenance intervals for individual components, thereby reducing the risk of breakdowns, increasing first-time-fixes and decreasing maintenance cost.

In a metro transit system, computers are widely deployed in on-board control and video recording systems. As space is very limited on refurbished rolling stock, computing systems are often installed at places that are hard to reach and maintain such as cabinets, compartments under passenger’s seats, or on the ceiling. Having ready access to a computer’s current condition (storage, CPU, memory) so that you can implement a preventive maintenance routine is an important aspect of ensuring a smooth transit system

The high financial and reputational costs of railway accidents and long delays have led railway infrastructure managers to adopt increasingly sophisticated preventive maintenance systems. However, the ability of railway operators and maintenance engineers to prevent costly system failures and optimize resource allocation depends on myriad real-time wayside asset condition information provided by separate monitoring systems. These data acquisition systems are often comprised of many sensors, transducers, and remote terminal units running on different platforms and closed communication protocols, which can make maintenance more challenging and costly.

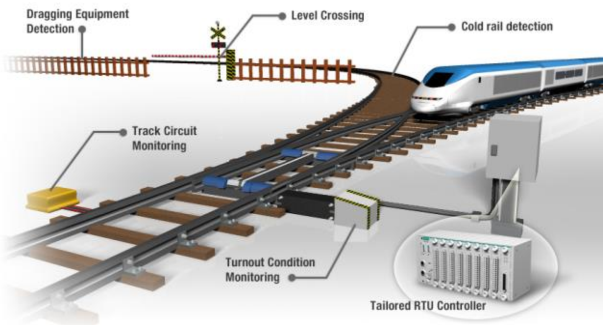


Figure 7 – Integrating wayside Monitoring System [17]

Costly system repairs following deadly derailments are not the only the reason why railway operators and infrastructure managers spend so much on track maintenance and renewal each year. As once said by Benjamin Franklin; “*An ounce of prevention is worth a pound of cure.”*

Even the Chinese Government, which received a great deal of criticism for overlooking safety in its push to develop the world’s largest high-speed rail network, has begun investing in safety-related monitoring improvements in the wake of the deadly 2011 Wenzhou high-speed train collision

According to the official Wenzhou accident investigation report, a piece of signalling equipment was severely damaged by a lightning strike just before the deadly accident. Thus, the railway signalling system erroneously informed the control centre that an occupied section of track was clear. Besides killing 40 passengers and injuring over 200 others, the Wenzhou derailment was also extremely costly for China and negatively affected the economy. Ultimately, Wenzhou highlights the importance of remote monitoring systems and maintenance procedures in ensuring reliability and controlling costs, financial and otherwise. As railway operators around the world have come to realize, having the right information at the right time is not only essential for preventing accidents, but can also lead to more optimal asset management and track performance.

Increasingly sophisticated condition-based maintenance systems are clearly becoming best practice in the railway industry to guarantee system reliability, availability, maintainability, and safety. At the same time, infrastructure monitoring for railway preventive maintenance includes many different subsystems that monitor myriad wayside conditions including, but not limited to, railroad turnouts and crossings, track geometry, and rolling contact fatigue. Each of these parameters provides information necessary for railway operators to prevent costly system failures and maximize efficient use of assets and equipment. [19]

5.4 Challenges in Transport

The arrival of “big data” is helping traffic control centres respond more quickly to accidents and backups, while helping individual travellers navigate their moment-by-moment decisions.

The greater challenge is to harness the extraordinary innovation taking place to make far more efficient use of the existing transportation system.

Intelligent mobility is the future of transport. It is about harnessing innovation and emerging technologies to create more integrated, efficient and sustainable transport systems. It marks an exciting meeting point between traditional transport and the new products and services that are emerging as we start to exploit vast amounts of multi-layered data.

6 SAFETY

Rail operators and infrastructure owners are very sceptical about the new telecommunication technology in the safety critical rail systems applications. Currently, there is some rail conversation happening regarding threats, cyber-security and network security. The biggest question remains: are the wireless, vital rail systems going to be safe? We hear every day someone’s computer was hacked. We are talking about the private users, however, just recently we all hear about a potential that hackers from one country influenced, or made impact on the election results in another country. Are we going to experience some problems with the introduction of CBTC or ETCS level II?

6.1 Threats

Early industrial control systems were designed for reliability rather than security, since there was no Internet to complicate the picture. Trusted components (sensors, controllers, workstations) were easy to connect. Components had no built-in security or communications protocols, interfaces were unprotected, and all users were assumed to be authorized. And the monolithic network architecture ensured that there were no security checks to impede transmissions. So, while such integration undoubtedly brings performance and operational benefits, it also opens the door to unforeseen hacks.

Some attempt was made to separate control networks from corporate networks using firewalls, but the design goals were still more concerned with reliability and cost reduction than with security. This might be described as ‘insecure-by-design’.

One major concern of converged networks is the emergence of a new class of threats that targets industrial automation systems. Often lacking security measures, legacy networks are particularly vulnerable to malicious network attacks or unintended operations. Once compromised, these legacy networks can become back doors that allow attackers and unauthorized personnel to gain access to the plant network from enterprise networks or other industrial networks

Analysing the known types of attacks over several years, the United States Computer Emergency Readiness Team identified a substantial list of common ICS vulnerabilities including:

Buffer overflow

Cross-site Scripting (XSS) – where a hacker inserts and executes malicious script inside a legitimate website or web application that the victim uses

Lack of proper access control and password policy

- Lack of data protection policy » No maintenance of Operating System (OS) » Outdated software utilization and poor patch management
- Lack of test facilities » Dual Network Interface Card (NIC) - two network cards as security between ICS and corporate systems » Lack of remote access security
- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) vulnerabilities
- Lack of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) • Clear (i.e. unencrypted) text utilisation
- Poor log maintenance
- Lack of proper anti-virus or malware Protection software – Kaspersky Lab.

While data protection is paramount, however, these measures only secure data transmissions from being read, or from DoS (Delivery of Service) or man-in-the-middle attacks - they do nothing to protect the physical hardware. Should that attack vector be left open then the entire system can be quickly compromised by even an inexperienced attacker. Fortunately, there exists Trusted Platform Computing, (TPC) a powerful tool that addresses this vulnerability, but which currently remains rather under-utilized in the industrial computing field.

6.2 Cyber-security

There are many protections in place today, mostly focused on the physical security of the passengers and the transit system’s assets. In general, any device that uses a digital processor, communicates with digital devices, connects to a communication network via a wired, or wireless connection, or that can be programmed could be considered for protection.

The conventional challenges of securing data across the open Internet, or over local wireless links—like 3G/4G cellular, or Wi-Fi—are easily addressed using readily available tools like packet filtering, firewalls, and data stream encryption with a VPN tunnel, or WPA2.

Cyber security is a collection of tools, policies, security safeguards, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organisation and user’s assets... [20]

The general security objectives comprise confidentiality, integrity, and availability. [20]

United Nations Information Technology Unit (2016) Definition of cyber security

Transit agencies have spent anywhere from dozens to more than 100 years running their systems and have dealt with a vast array of issues and threats with an excellent record of safety, on-time performance and reliability. The challenge today is to add cybersecurity awareness and cyber defence measures to the transit agency culture in the same manner that safety has been added to the culture of manufacturing and transportation. This will reduce the risks to transit agencies and their supplier base from cybersecurity incidents and possible liability should an incident take place.

Until recently, the security of control systems could be addressed by carefully limiting physical access to elements of the control system, such as modems, terminals and control computers, and relying on obscurity.

Railway Networks may be subject to unauthorised access through various means…..

Remotely, via the Internet, or unsecured telecom networks

At close hand, through direct contact with infrastructure (e.g. through a USB port)

- Locally, through unauthorised access to physical infrastructure, or insider threat (infiltration).

These vulnerabilities are weaknesses in control systems, information systems, system procedures, controls, or implementations that can be exploited by a threat source.

There is potential for cyber-attacks to cause damage and loss to rail networks. Successful cyber-attacks could result in: [20]

- threats to safety
- disruption to the rail network or services operating on it
- economic loss to rail operators, suppliers or the wider UK economy
- reputational damage to rail companies or the UK economy
- loss of commercial or sensitive information from the rail industry or suppliers
- criminal damage.

The role of cybersecurity is to ensure that these existing systems cannot be duped into making a wrong decision, and to ensure that these systems cannot be directly controlled by anyone other than their owner/operator. Another goal is to reduce the likelihood of human error, such as forgetting to apply an update or applying an incorrect update to a part of the system.

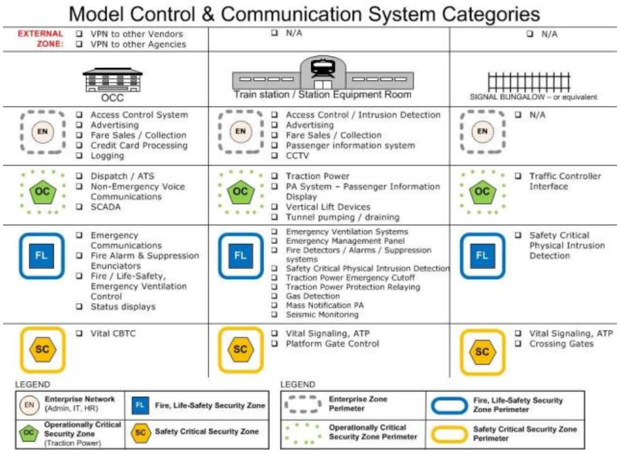
Just as transit agencies have created a safety-centric culture—saving lives and reducing accidents and accident severity—they need to foster and create a cybersecurity culture. This requires an awareness program; a training program; an assessment of cybersecurity threats; a reduction of the attack surface (the number of places and ways someone can attack transit systems); a cybersecurity program that addresses: threats, mitigations, the software/firmware update process, monitoring and detection methodologies; and the ability to be audited to check for compliance via logs and change-management systems.

6.3 Network Security

A communication-based train controller (CBTC) is a train's automatic control system based on a Digital Command System (DCS) architecture. Because of recent advances in wireless transmissions, CBTCs now rely heavily on WLANs to ensure constant train-to-ground data connections. The best way to avoid a link failure on a WLAN is through redundancy, which ensures that clients remain "always on" and allows critical network links to continue to transmit data. WLAN products support Ethernet redundancy using Rapid Tree Spanning Protocol (RSTP) and power redundancy using dual DC inputs and Power over Ethernet (PoE). These multi-redundant features guarantee that the DCS system can provide uninterrupted robust seamless mobility, and ensure that safe and secure communication will always be available to meet the demands of video, voice, and other bandwidth-demanding applications, such as maintenance tasks and passenger information systems.

Seamless roaming handover with a complete redundant Digital Command Systems (DCS) architecture provides reliable and sustained communication for smooth CBTC operations. Train-to-ground links are based on a radio frequency communication network that provides a connection between each client on the vehicle and an access point linked to the wayside network. There are several differences between a rail transportation system and a single manufacturing site:

A rail system covers vast distances, and each segment of the rail system must communicate with its adjacent segments and with the operations control centre (and backup operations control centre). Transit agencies are expert at the physical security aspects of their systems. Cybersecurity adds a new dimension to the security program.



Model Control & Communication System Categories

	OCC	Train station / Station Equipment Room	SIGNAL BUNGALOW – or equivalent
EXTERNAL ZONE:	❑ VPN to other Vendors ❑ VPN to other Agencies	❑ N/A	❑ N/A
EN	❑ Access Control System ❑ Advertising ❑ Fare Sales / Collection ❑ Credit Card Processing ❑ Logging	❑ Access Control / Intrusion Detection ❑ Advertising ❑ Fare Sales / Collection ❑ Passenger information system ❑ CCTV	❑ N/A
OC	❑ Dispatch / ATS ❑ Non-Emergency Voice Communications ❑ SCADA	❑ Traction Power ❑ PA System – Passenger Information Display ❑ Vertical Lift Devices ❑ Tunnel pumping / draining	❑ Traffic Controller Interface
FL	❑ Emergency Communications ❑ Fire Alarm & Suppression Enunciators ❑ Fire / Life-Safety, Emergency Ventilation Control ❑ Status displays	❑ Emergency Ventilation Systems ❑ Emergency Management Panel ❑ Fire Detectors / Alarms / Suppression systems ❑ Safety Critical Physical Intrusion Detection ❑ Traction Power Emergency Cutoff ❑ Traction Power Protection Relaying ❑ Gas Detection ❑ Mass Notification PA ❑ Seismic Monitoring	❑ Safety Critical Physical Intrusion Detection
SC	❑ Vital CBTC	❑ Vital Signaling, ATP ❑ Platform Gate Control	❑ Vital Signaling, ATP ❑ Crossing Gates

LEGEND

EN Enterprise Network (Admin, IT, HR)	FL Fire, Life-Safety Security Zone
OC Operationally Critical Security Zone (Traction Power)	SC Safety Critical Security Zone

LEGEND

Enterprise Zone Perimeter	Fire, Life-Safety Security Zone Perimeter
Operationally Critical Security Zone Perimeter	Safety Critical Security Zone Perimeter

Figure 8 – Model Control & Communication System Categories

Cyber security measures and procedures considered appropriate are those that focus primarily on terrorists, hackers, hacktivists and cyber criminals, and deliver value for money. Resilience should be considered to comprise but not limited to the following….

- Reduction on the likelihood of attack, through good multi-layered design (defence in depth) and robust operational and maintenance procedures, with consideration given to the defence-in-depth principle, single points of failure and the role of noncyber related fail safes

Mitigation against disruption and failure once systems come under attack, through development, testing and maintenance of robust contingency plans

Management and monitoring of the effectiveness of systems and procedures, to ensure optimum performance, and early warning of attack

- Contingency, recovery, and continued operation of the rail network.

6.4 Some Future Predictions

Cyber security is a major concern for rail operators as they open their networks as part of the IIoT to facilitate access to and from public networks. Manufacturers around the world are dedicating a lot of time and effort to build higher security in IIoT products and solutions. However, an end-to-end security solution eludes the IIoT industry, leaving the operators to their own devices when it comes to dealing with the increasing number of cyber-attacks.

To prevent system intrusions and attacks, it is essential to have a good user access control mechanism in place that can identify, authenticate, and authorize users. Compliance with cybersecurity standards, such as the IEC 62443-4-2 standard constitutes a series of reports, and other relevant documentation that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). Implementing multiple levels of authentication based on established best practices in the industry can help secure your IIoT applications.

On the device side, a stricter access control mechanism based on user account, password, and key authentication, and better management of the authentication interface can help prevent cyber-attacks. Organizing devices into groups and granting access privileges to only certain users, or user groups based on their roles is a good way to prevent unauthorized access of devices on your network.

The key is to strike the right balance between accessibility and security. Both the degree of uncertainty and the rising number of known incidents are red flags calling for the dedication of greater resources to monitoring, detecting and analysing anomalous activity in control system networks. Breaches of security that do not disrupt normal operations may still be detected, if trained and knowledgeable personnel armed with the requisite tools look for such breaches.

Rapid detection is key, because the longer breaches remain unknown, the greater the potential impact. Due to the critical nature of many control systems, the documented rise in attacks on these systems shows the potential impact of even brief operational disruptions.

SCADA StrangeLove, a group of cybersecurity researchers, has demonstrated the flaws in a certain number of the components that make up the so-called « smart » trains.

Their operation shows how intruders can use a single flaw to access all components on a train. European trains are controlled by the **SIBAS system**. Although this system is deemed safe, the WinAC RTX controller, one of the SIBAS' components made by Siemens, is said to be a security vulnerability. Breeches in the different systems make the computers controlling the trains extremely exposed. Another example of a potential system under threat is the CBI, that enables a train to start its journey correctly and to avoid collisions. SIM-GSM cards are another component questioned by SCADA StrangeLove researchers. These cards are used to geo-position trains. However, the cards can suffer from connection breakdowns leaving the train to its own devices, with minimum protection, and prone to mobile attacks on its modem.

Attacks against a modern train's components constantly challenges cybersecurity. Attackers can exploit even the slightest flaws that can be found in IT systems. With an attack lasting just a few seconds, a poorly prepared company that is unable to address the problem can expect to suffer for a long time. [21]

7 CONCLUSION

The incredible pace of technological change in transportation makes it difficult to forecast the future with accuracy. However, trends point to intelligent, more integrated systems for moving passengers and freight.

Machine-to-Machine (M2M) technology will increase efficiency by using sensors embedded in a wide array of objects and systems to automate tasks and deliver real-time analysis and monitoring. Increases in computer power and the ability to handle the processing of large amounts of data in real time. This will lead to more effective use of Big Data and the Internet of Things will allow transportation modes to communicate with each other and with the wider environment, paving the way for truly integrated and inter-modal transport solutions.

Rail stations will become destinations and lifestyle centres that further blend our commute with our lives. People are increasingly using stations, not just as places to catch a train, but as centres for leisure and business. [22]

1. Cyber-security plays an extremely critical role when the wireless rail systems are in operation

   All parts of the traditional transport sectors realise that cyber security is a risk affecting their industry, and they need to work to tackle the issue. But the maturity of capability is variable, and there is little evidence of an intelligent mobility approach to cyber security.

   Sector vulnerability and cyber threats are evolving. Just like the technology changes, the threat landscape facing those in the intelligent mobility space is also changing. Cyber criminals are rapidly adopting new technologies, and refining the cybercrime business model. Attacks in this connected world will be possible from anywhere, at any time.

2. Big data creates an enormous opportunity in asset management There is every reason to believe that GPS-based data, along with enhanced instrumentation and communications, can lead to more efficient equipment utilization on railways. It is not much of a stretch to imagine a combination of GPS data with on-board performance data feeding through high capacity communications to system

wide computers to yield much more efficient use of railway capacity, with a related impact on the competitive position of railways in both freight and passenger markets. This could also lead to increasing automation ("intelligent autonomous vehicles") that would lead to improved safety and potentially more efficient use of labour.

Examples of driverless passenger trains include the automated systems in operation in Copenhagen, Paris, Singapore, Dubai and São Paulo. Automated systems optimise the running time of trains and increase the average speed of the system, allowing more trains to operate closer together, reducing the time it takes a train to slow down at stations, and increasing reliability. The Dubai Metro is the longest driverless metro network in the world, spanning 75km. The Copenhagen Metro was one of the first to feature a fully automated system, including depot operation and launching, and operates 24 hours a day.

3. Digital connectivity

It's important to understand how changing consumer expectations will affect their decisions about choosing how to travel from place to place. Global companies such as Amazon and Netflix have shaped and defined current consumer expectations. Travelers will expect to be able to search, book and amend their trip in minutes from their mobile or tablet. Voice activation is also seen as an opportunity for rail operators to offer a more simple and intuitive booking experience.

The combination of the Internet, which holds the world's knowledge; wireless, which gives us ubiquitous and low-cost access to it; and smartphones that make our interfaces portable and cheap, is transformational.

Today's traveller expects to receive a level of service that understands their individual needs and preferences. In this respect, rail is still playing catch up, but operators are catching up quickly.

Transport consumers of the future will not demand individual elements of mobility at a time, they will demand products that combine and enable automation, new mobility models, and smart ecosystems. This scaled-up demand also scales up sources and opportunities for cyber-attack over and above the current industry-specific focus.

The future of railways with Big Data and the Internet of Things will allow transportation modes to communicate with each other and with the wider environment, paving the way for truly integrated and inter-modal transport solutions by Arup Report. [23]

The desired future for rail requires a bold vision and a strong will to implement change on the part of governments, the rail industry and those training the rail engineers of the future.

8 LITERATURE

[1] Brisbane Courier Mail, 30th May 2016

[2] G. M. Shafiullah, A. Gyasi-Agyei, P. Wolfs, "Survey of wireless communications applications in the railway industry", in AusWireless 2007: Proceedings of the Wireless Broadband and Ultra Wideband Communications 2007 International Conference, IEEE, Piscataway, N. J., pp. 65-70

[3] "A Roadmap for Digital Railways", http://www.cer.be/sites/default/files/publication/A%20Roadmap%20for%20Digital%20Railways.pdf, last accessed in January 2017

[4] Deloitte, Transport in the Digital Age, Disruptive Trends for Smart Mobility", March 2015

[5] The European Rail Research Advisory Council (ERRAC), "Strategic Rail Research and Innovation Agenda", October 2014

[6] R. El Hattachi, J. Erfanian, "NGMN 5G Initiative, 5G White Paper", February 2015

[7] D. Pisinger, "Robust Railway Operations – A big data challenge", DenBaneDanske Konference, 5th May 2015

[8] The Parliamentary Office of Science and Technology (7 Millbank, London SW1P 3JA, th UK), "Big and Open Data in Transport", PostNote, Number 472, July 2014

[9] H. Poonawala, V. Kolar, S. Blandin, L. Wynter, S. Sahu, "Singapore in Motion: Insights on Public Transport Service Level Through Farecard and Mobile Data Analytics, June 2016

[10] P. Hughes, "Making Big Data Risk Analysis work for the GB Railways", Big Data Risk Assessment research team, Institute of Railway Research, University of Huddersfield, September 2016

[11] ORACLE, "An Enterprise Architect's Guide to Big Data", Reference overview, ORACLE White Paper, March 2016

[12] World Economic Forum, "Industrial Internet of Things: Unleashing the Potential of Connected Products and Services", in collaboration with Accenture, World Economic Forum, January 2015

[13] T. H. Davenport in Big Data in Big Companies

[14] Rail Cyber Security guidance to industry – RSBB

[15] Moxa, White Paper – Fast Rolling Stock Roaming

[16] C. Arnold, J. Mocki, "Modelling Payload Capacity using common software applications as applied to a Rail Utility's Telecommunication network", 2017

[17] Moxa, White paper – Integrating wayside Monitoring System

[18] Railway Assets: a Potential Domain for Big Data Analytics Aug 2015

[19] Moxa, White Paper – Implementing passenger Wi-Fi networks

[20] President's Council of Advisors on Science and Technology, "Big data and privacy: a technological perspective", report to the President of United States, Washington, D.C. 20502, May 2014

[21] Cyber Security: Trains now in firing line of the hackers. Senryo used cases

[22] Amadeus Rail – Reinventing Rail in Europe – The battle for the customer

[23] ARUP the Future of Rail 2050

[24] Roadmap for Digital Railways – Railway Gazette 2016

AUTHORS

Nick Czeperko

Nick Czeperko has over 30 years of experience working in the industrial telecommunications industry. He started his career as a qualified electrician designing and installing industrial control switchboards, before founding several electrical engineering installation and design companies.

He quickly recognised the emergence of M2M (Machine to Machine) communications and the transition of Ethernet communications into the industrial process control market.

As General Manager of Ethernet Australia Nick helps customers across industries and sectors to solve complex industrial communications tasks whether it is asset tracking and monitoring, preventative maintenance, controlling production lines, monitoring traffic systems, or controlling power distribution.

Nick helps companies to use industrial communications to improve efficiency and processes by having analytical data at their fingertips. He can help customers to save time and money with preventative maintenance scheduling and achieve greater life from their industrial investment.

He has developed a solid supply chain from various overseas manufacturers from countries such, as Taiwan, China, various parts of Europe and USA.

He is business development specialist with expertise in negotiating and managing national and international supply chains, and managing and overseeing the technical and sales teams.

Specialties, General Management, Business Relationship Management, Business leadership, National & International supply and customer chain management, budget forecasts, understanding company structures, utilising commercial and financial reporting mechanisms.

Jacek Mocki

Jacek is a qualified, chartered, transport engineer, highly experienced as demonstrated through his career spanning:

- Government: railway infrastructure manager, consultancy including Ministerial consultation and briefings;
- Private Industry: consultancy, concept design and investment / business case preparation, projects – design, procurement, construction, installation and commissioning, operations – asset management, including new product and upgrades introduction, asset renewals management and computerised asset management tools introduction, project management as well as business development management and direction.

Between 2000 and 2005, Jacek was heavily involved in some key European Union projects in the UK and in Poland.

First time, he worked on Australian railway infrastructure in Victoria in 2004, taking part in a review of the Metropolitan Melbourne Railway Infrastructure. Since then he was involved in the following key projects: NSW Train Order Working Implementation Plan and North Coast Loops Extension; QLD Corinda Darra Rail Upgrade, QLD Redbank WESTLOCK, QLD FAdC/WESTRACE II introduction, QLD Herbert Street Level Crossing and QLD Points Condition Monitoring.

Currently, he works for MOTZKY Pty Ltd addressing the customer’s needs in three major categories: Innovation for cost reduction, Optimise asset usage and Infrastructure investment efficiency. At MOTZKY, Jacek developed an innovative delivery methodology - ACS that is successfully utilised in customers’ and MOTZKY’s projects to achieve predictable outcome.