Smart Transport, Smart Security

Improving the cybersecurity and resilience of smart transport

Dr. Malcolm Shore

Cybersecurity Officer

Huawei Technologies | Australia

April 2018

HUAWEI

Table of Contents

Executive Summary 1

1 Smart Transport – A Coming Revolution 2

1.1 What do we mean by Smart Transport? 2

1.2 Why transport will be smart – the value proposition 2

1.3 Smart Transportation Framework 4

1.4 Current and future network architectures 5

1.5 Smart connectivity 5

1.6 Vehicle Automation 6

2 Describing the Smart Transportation Architecture 7

2.1 Infrastructure 7

2.2 Traffic management 7

2.3 Logistics Management 8

2.4 Individual mobility management 9

2.5 Vehicle 9

2.6 e-Payment 10

2.7 Data 10

2.8 Safety and Security 10

3 Cyber Threats and the Need for Resilience 12

3.1 Threats 12

3.2 Resilience 12

3.3 Changing the perception of technology security 14

3.4 Huawei's insights into IoT security 14

4 Cyber Security Standards 16

4.1 Security standards, frameworks, and controls 16

4.2 Cyber Essentials 17

4.3 NIST Cybersecurity Framework 18

4.4 ITU X.805 19

4.5 ETSI NFV-SEC003 Network Function Virtualization (NFV) Security 19

4.6 ITU X.SDNSec 19

4.7 ETSI TR 102 940 ITS security architecture 20

4.8 Security evaluation specifications 21

5 Case Study: Digital Rail 23

5.1 Developing a smart transport security approach 23

5.2 Conceptual solution 23
5.3 Addressing the cyber threats 23
5.4 Detecting and protecting against cyber attack 25
5.5 LTE and backhaul security services 25
5.6 Application security services 26
5.7 An advanced security architecture to support smart transport 27
6 Case Study: Digital Rail 29
6.1 The smart security architecture for digital rail 29
6.2 Security design considerations 30
6.3 Security controls 31
7 Conclusion 32
7.1 A smart transport security architecture for the future 32
7.2 Huawei and smart transportation cybersecurity 32
APPENDIX 33
NIST Cybersecurity Framework Digital Rail 33

Executive Summary

The potential for economic benefits from the internet of things is enormous, and can be seen in the early development of smart transport solutions. Benefits are already accruing from driverless trucks being used in mining, and smart telemetry on digital rail solutions. However, the real impact is yet to come. We may within five to ten years see driverless cars have as big an impact on society as did the transition from horse-drawn carts to automobiles. Driverless cars and their associated services will be a trillion dollar industry, and will lead to economic gains in a wide range of other industries.

But businesses around the world are struggling to maintain the security and safety of their technology systems and network infrastructures. There are too many vulnerabilities, too many cyber criminals, and too few cyber security resources. Incidents such as taking over a cars telematics while it's driving on the highway and hacking into an aircraft's network through its entertainment system provide demonstrations of vulnerabilities and highlight the need to provide smarter security solutions to match the smart technology that is being developed for the transport sector. The baseline for any technology should be secure software engineering, building security into all technology designs through best practice processes, tools and techniques. This has never been more pressing than with the imminent explosion of the internet of things.

Huawei is a leading provider of smart transport solutions and has invested many years of effort into developing its own framework for cybersecurity across its people, processes, and technology. The result of this is a set of products which are amongst the most secure in the industry, and services which incorporate robust controls for cybersecurity to ensure the protection of its customers' networks and information. Huawei is committed to contributing to the improvement of cybersecurity across the transport industry through deep collaboration and participation in open forums such as standards making bodies. Huawei has established a number of open labs around the world to enable collaborative research and development.

This White Paper provides further open contribution by Huawei to the improvement of the cybersecurity and resilience of smart transport solutions.

John Suffolk.

John Suffolk

Global Privacy & Cyber Security Officer

1 Smart Transport – A Coming Revolution

1.1 What do we mean by Smart Transport?

There is no one definition that has been agreed as to just what the term Smart Transport covers. In 2010, the European Union defined Intelligent Transportation Systems (ITS) as a systems "in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport." ENISA has defined intelligent transport as "The application of information and communications technologies to transport so as to improve levels of safety and efficiency"[1].

The term smart transport brings may bring to the public mind a vision of driverless cars but the application of smart technologies into the transportation sector is much wider than that. We're seeing smart technology appear in urban streets and on highways. The trucking sector has invested heavily in smart fleet solutions. The mining industry is undergoing a significant transformation through the introduction of numerous smart mining technologies for carrying out mining operations, and a significant part of this is the use of autonomous mining vehicles with advanced real time monitoring and analytics software providing major improvements in safety, cost efficiency and productivity. Smart logistics for shipping is delivering significant cost savings, as are digital rail systems. Drones are an embryonic addition to the smart transport sector, with companies such as Amazon looking to use them for goods delivery. The term "smart transport", then, covers not only smart vehicles of all types but also intelligent transport systems and innovative applications that take advantage of the connectivity and data that characterizes the smart environment.

Huawei's X Labs has researched the smart transportation sector and designed a framework comprising six transportation domains[2]. These provide a functional architecture with which to look at the full eco-system of products and services required to deliver and support the full range of smart transportation solutions.

1.2 Why transport will be smart – the value proposition

The development of smart transport solutions is considered a significant driver for social progress, allowing people to interact more effectively and enabling more efficient transportation of goods around the world. Currently smart transport solutions are being used in niche areas such as autonomous mining or automated commuting systems but have yet to have significant impact on society and the economy. However, the potential exists for the global smart transportation ICT market to triple over the next five years as it increasingly becomes part of day to day life.

The value of smart transportation systems is already being realized commercially and at scale. Intel worked with TransWiseWay, a telematics and service provider, to deploy a connected commercial vehicle solution in China[3] in 2014. This solution delivers higher reliability, improved safety, and access to real time travel information for the commercial fleet, and uses a mix of 3G, 4G, WiFi, and wired networks as well as a variety of sensing

[1] Cyber Security and Resilience of Intelligent Public Transport, ENISA December 2015

[2] Smart Transportation: Maximize mobile network's value beyond connectivity, X Labs 2016

[3] Building an Intelligent Transportation System, Intel 2014

technologies. It had over a million connected vehicles in 2015 and will eventually support 10 million vehicles.

6-12% of GDP

In many developed countries, transportation accounts for 6-12% of GDP

10-15% of HOUSEHOLD COST

On average, transportation accounts for 10-15% of household expenditure.

8% OF DAILY LIFE

Transportation impacts everyone's life. On average, people spend 8% of their time commuting to and from work.

The transport sector is a significant cause of deaths and injury: approximately one million people die in traffic accidents every year[4], and we can add to that the cost of rail and air disasters. The evolution of transportation solutions has resulted in an increased focus on safety, from the adoption of sensor-based crash mitigation measures to real time telemetry for vehicle maintenance and driver monitoring. However, smart transportation has the potential for a much safer future.

Vehicle emissions have been one of the major contributors to global warming, and traffic congestion has a major impact on productivity and quality of life. Jakarta is one of the most congested cities in the world[5], with commuters spending up to four hours in traffic not being unusual. These issues can all be directly or indirectly mitigated by well-designed smart transport.

The now ubiquitous nature of the internet is driving innovation. This is visible in the many facets of connected technology which together are known as the internet of things. Studies indicate that for every point measured on the Global Connectivity Index[6], there is a 2.3% improvement in economic productivity. Progressing from ubiquitous internet to ubiquitous connectivity will lead to a revolution in the way we live our lives, the way we work, and the way the nation prospers. Smart cities are now being built with highly connected infrastructure, and highly automated transportation services. We are now seeing autonomous vehicles being increasingly used in industry, and driverless cars will soon be a commercial reality.

Car connectivity and autonomous driving are hot topics both within and outside of the car industry as strategies emerge to remove the potential for human error which causes many of the road accidents, with a flow on benefit for increased productivity and well-being, and reduced healthcare costs. These capabilities will also allow commuters to work or enjoy leisure time while travelling, further improving productivity and increasing quality of life.

Advanced fleet management solutions are an important area of focus for smart transport. Smart sharing and smart routing solutions have the potential to dramatically reduce or remove congestion and reduce fuel usage, and online engine telemetry can drastically reduce maintenance costs. The potential in reducing congestion alone has been estimated as a saving of 0.8% of GDP[7].

[4] Global Status Report on Road Safety2015, World Health Organisation 2015

[5] https://www.theguardian.com/cities/2016/nov/23/world-worst-traffic-jakarta-alternative

[6] "Global Connectivity Index 2016 White Paper", Huawei 2016

[7] "The cost of traffic jams", The Economist, 2014

The surging nature of public transport demand causes peak time overcrowding on buses and trains, and this makes public transport as we know it an imperfect solution. Strategies are being developed for smarter solutions to address these issues[8]. Smart phone applications and the provision of real time data feeds can improve the traveller experience and allow more informed decision making. Early disrupters such as Uber have demonstrated the ability for significant improvement in the consumer transport sector. More reliable vehicles have reduced the amount of on-road breakdowns, and in-car navigation systems have improved routing.

The emergence of connected smart city/smart transport solutions have brought us to the verge of a major revolution in consumer and business transportation services, and major changes in city infrastructure. Cyber security will be one of the keys to its success.

1.3 Smart Transportation Framework

Smart transport is not just an economic initiative for individual businesses, it's a shared opportunity for government, business and society to benefit from the new internet of things technology. To achieve maximum benefit, it requires collaboration between national and local governments and their infrastructure providers to deliver more efficient services while better meeting the demands of enterprises and individuals.

Collaboration at this scale needs to occur across a large number of diverse and independent projects. This requires a common set of outcomes are agreed and a common framework exists to deliver to those outcomes. Having a common framework for smart transportation provides the ability to start with limited scope commercial initiatives which can contribute to the longer term smart transport solutions and to smart city infrastructure development.

Figure 1: Huawei Smart Transportation Framework

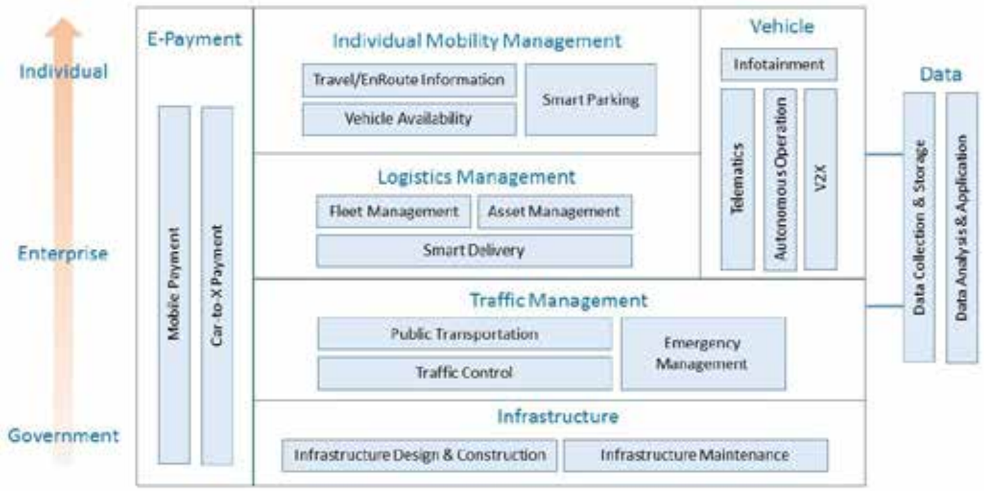


Figure 1 depicts Huawei's framework[9] for smart transport applications, with key subsystems shown for each of the six domains: Infrastructure, Traffic Management, Logistics Management, Individual Mobility Management, e-Payment and Vehicles.

[8] http://theconversation.com/the-smart-future-of-public-transport-1815

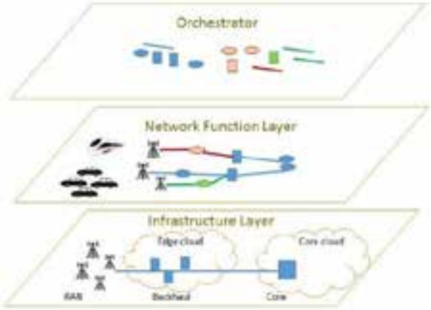
[9] Smart Transportation: Maximize mobile network's value beyond connectivity, X Labs 2016

1.4 Current and future network architectures

One of the key components of smart transport will be the services which connect vehicles to other elements of smart transportation. Smart transport needs connectivity, from the near field solutions which enable people to interact with in-vehicle systems to the mid-range connectivity from the vehicle to the infrastructure, and then to remote connectivity to and from the vehicle. In networking terminology, the vehicle sits in the access layer as a device connected through proximity and backhaul transmission to the core network, and then through to the application services. This end-to-end view is a significant area of focus for the security architecture.

Traditional 3G and 4G carrier solutions have used a three layer infrastructure of management, control, and user plane which delivers network services and applications, as described the ITU X.805[10] standard. With a move to 5G, a new architecture is emerging in which the key focus is on providing multiple virtual networks to deliver heterogeneous end-to-end services each with its own network characteristics. This is exactly the architecture required to support smart transport, with its demand for large numbers of connected vehicles, concurrent real time high bandwidth infotainment and narrowband telemetry channels. While initial deployments of smart transport will use 4G NB-IoT, 5G with its NB-IoT slices will quickly become the target network for integrated services as the smart transport sector matures.

Figure 2: 5G Architecture



In order to deliver an integrated set of heterogeneous network services, 5G approach provides virtual network functionality (VNF) which can be orchestrated through software defined networking (SDN) to use the resources in the traditional radio access, transmission, and core segments of the network infrastructure layer. These resources will form dedicated business driven logical networks, otherwise known as network slices, which provide the end-to-end service for the user. This is one of the largest and most far reaching transitions underway in the telecommunications sector, and is based on specifications being developed by more than a dozen standards bodies. Huawei is a leading contributor to those standards.

VFN/SDN shifts how an operator designs, develops, manages and delivers products and services to achieve technological and operational efficiencies. These benefits are aimed at fundamentally redefining the cost structure and operational processes, enabling the rapid development of flexible, on-demand services and maintaining a competitive position.

Huawei has developed an ICT functional converged reference architecture for 5G which incorporates end-to-end network slicing and security, decoupling of the RAN and core, functional decomposition which separates the central and distributed units of the radio access network and separates the control and data plane in the core, and delivers agile operation. This provides a simplified and automated business model.

1.5 Smart connectivity

[10] ITU Recommendation X.805 Security architecture for systems providing end-to-end communications

There are three distinct connectivity solutions required for smart transportation: entertainment services, connections to other vehicles and the environment, and telemetry connections to remote services including the connectivity that supports autonomous driving.

Discrete per-function vehicle information displays have given way to connected infotainment systems, and DVD and streaming video players, in-car navigation, and touch screen passenger display. With the high demand for internet connectivity that has developed along with smartphone technology, vehicles require broadband internet connectivity for their infotainment solutions, and in-vehicle WiFi services are becoming popular.

The use of reversing sensors and cameras to avoid collisions is the first stage of fully crash-avoidance systems, which through various means of connecting with other vehicles and the environment can sense and plan around situations which may, in a human-driven world, introduce the risk of collision. This connectivity comes from what are known as V2X solutions – Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Pedestrian (V2P).

Remote connectivity to telematics has already arrived on the market. Some vehicles offer performance monitoring with real-time transmission back to the servicing center, in order to detect any problems and provide early maintenance. Remote slowdown and stop capability also exists to enable law enforcement agencies to better manage pursuits. Remote vehicle location has proved invaluable for precise tasking of emergency services in responding to accidents.

Smart transportation will be supported with a range of network solutions, from narrow band IoT (NB-IoT) for telemetry to high bandwidth streaming IP entertainment services, making 5G a key technology for the longer term smart transportation vision.

1.6 Vehicle Automation

The implementation of automatic pilots in aircraft is a step away from delivering a fully autonomous aircraft. Remote piloting is already being used for military drones, and Boeing and Airbus are running trials with autonomous airliners. The mining industry has for some years now been using autonomous trucks. Autonomous train operation and driverless trains are now a reality, and these are seeding a new industry of driverless people movers for in-city use.

There is a lot of popular interest in driverless cars. There is also commercial interest from companies such as Uber to deploy them not only as taxi replacements but also as consumer car replacements. With trials notching up many tens of thousands of kilometers already, these are on the verge of commercial scale production.

Regulators are already preparing for driverless cars, with the US National Highway Safety Administration describing four levels of vehicle automation, ranging from Level 1 automation of individual functions, to level 4 in which all safety related functions are automated. As the level of autonomy increases, the level of connectivity also needs to increase to achieve the benefits of safety and quality of life experience. The emergence of V2X standards from 3GPP and the evolution of cellular communications to 5G will be critical enablers to support advanced smart transport solutions.

2 Describing the Smart Transportation Architecture

2.1 Infrastructure

The foundation of smart transport architecture in Figure 2 is the infrastructure. The transportation infrastructure starts at the local level with urban roads and extends to the national highways and transport services in and out of the country. The municipal governments, the regional authorities, and the national government all have their part to play in delivering and operating the transport infrastructure. Smart transportation solutions are in the main delivered incrementally with infrastructure upgrade projects, through annual improvements as well as smart city projects.

The transportation infrastructure also includes industrial infrastructure. Wireless connectivity is used in the mining sector to deliver improved safety and productivity, and this will continue with new network technologies providing improved coverage of mining operations. Huawei has fielded a number of NB-IoT and eLTE solutions to achieve this, and will improve upon these solutions with its 5G technologies.

Smart infrastructure needs to be reliable and responsive, and it will be a prime target for cyber attack. It will need to be able to detect malicious activity from the many inputs it receives and have the capability to shut down non-critical functions should such an attack have any significant impact. This level of resiliency survivability will be a defining characteristic of successful solutions and will be key to delivering safe transport solutions.

2.2 Traffic management

Traffic management in Figure 1 has three components: public transportation, traffic control, and emergency management.

Public transportation revolves around bulk movement of people from a limited number of pickup points and this model is likely to continue to dominate smart public transport services for the foreseeable future. The use of autonomous public feeder vehicles providing home pickup to link to public transport systems – be they road, rail, sea or air - will likely extend the reach of the public transportation service and reduce the need for private smart vehicles and taxis. Smart ticketing systems will support use of smart public transportation, and this subdomain will also cover demand responsive transport and shared mobility systems. Smart public transport will be safe, convenient, and efficient.

Traffic management systems are an important facet of smart transport, interacting with and managing routing of smart vehicles. From speed control and vehicle routing to traffic light control, good traffic management is a priority for transportation. Smart traffic systems can improve current performance through continuous connectivity and seamless handoffs in the urban centres and on high speed roads. Current traffic control systems can be improved through vehicle to vehicle communications, vehicle to infrastructure connectivity and central planning of routes and speeds for all vehicles.

Achieving seamless connectivity at speed will be a key success factor for smart transportation, and 5G wireless technology will be an important part of that solution. Smart traffic systems need high speed real time data analysis, with sensors in and along the road providing rich data on traffic type and density. The use of smart poles for street lighting provides the infrastructure to enable two way communications between vehicle telematics systems and the metropolitan infrastructure. With autonomous vehicles and real time connectivity, smart cities can look to a future where there is no requirement for maintaining a costly traffic light infrastructure.

Digital rail systems with their low power consumption and efficiency can deliver an effective bulk transportation service, and high speed bullet trains are increasingly able to compete with air travel for inter-city passenger business. In both cases, better communications, more effective telemetry, remote monitoring, and autonomous control can deliver the level of safety required for high speed passenger trains and freight. Real time connectivity with moving block signalling allows more trains to be on the network at the same time. The use of telematics data collection and analysis provides opportunities for fault prediction and so more cost effective maintenance. From a business perspective, this all translates to more trains, better connections, lower costs and greater reliability. Ensuring safety requires the ability to handle real time data streams and respond accurately in real time.

Emergency management services are used heavily in support of crash response, and while the demand for these services should reduce dramatically with the evolution to smart transportation, emergency response will continue to be required. Smart transport can improve response effectiveness through automatic notification of incidents and real time monitoring of patients en route to hospitals.

2.3 Logistics Management

Logistics Management has three major functions: fleet management, asset management, and smart delivery.

Fleet management is an area where there is an immediate benefit from connectivity. Driver assisted vehicles, driverless vehicles, and in-vehicle engine monitoring all offer significant savings on fleet operations. The use of embedded mobile internal and environmental audio and video recorders/transmitters can provide benefits such as two-way audio, status indication, and panic alarms. This data can be instantly uploaded to the intelligent transport platform for centralized control and management. GPS real-time monitoring with route replay can enable rapid response to incidents such as breakdown, accidents, and hijacking. Smart law enforcement fleet management solutions will offer integrated connectivity with law enforcement databases, and smart taxi fleets will provide integrated dispatch. Smart transport fleets will make distribution much more effective and lower maintenance costs, while offering more reliable stock delivery and hence lower the cost of stock holdings. Many of the bigger trucking rigs now have autonomous capability, although drivers continue to be used.

Smart asset management is about the timely management of the cars, trucks, ships, aircraft, and rolling stock involved in the transport business. Continuous monitoring plays a part in achieving this, as does remote real-time telemetry. Maintenance of the fleet is enhanced by predictive monitoring and vehicle use profiling.

Maritime shipping solutions are another area of significant value for smart solutions, and one of the important smart asset management and delivery solutions is the Smart and Secure Trade Lanes (SSTL) industry initiative[11] which defines a baseline infrastructure that provides real time visibility, physical security through non-intrusive automated inspection and detection alerts. It uses a variety of wireless techniques, including RFID and satellite tracking, sensors and biometrics and focuses on container identification, scanning, tracking, and integrity as well as integration with transportation intelligence systems. Cybersecurity

[11] https://ec.europa.eu/taxation_customs/general-information-customs/customs-security/smart-secure-trade-lanes-pilot-sstl_en

will play a significant part in ensuring the success of the end-to-end tracking of containers particularly by ensuring records cannot be interfered with while goods are in transit.

2.4 Individual mobility management

Individual Mobility Management has three components: travel/en-route information, vehicle availability, and smart parking. These are all part of a wider category of smart city services to support travellers. The smart city will provide smart parking buildings and meters, fuel/charging stations, smart booking services for entertainment, hotels and restaurants, in-ground induction charging, and breakdown recovery services in support of the traveller. The smart road will deliver vehicular e-Payments for tolls and ticketing.

Individual mobility management is an area which has the potential for many innovative and interesting solutions to be developed. Their success will depend very much on whether adequate privacy protection is part of the solution.

2.5 Vehicle

Smart vehicles already have infotainment and advanced telematics, and more V2X services will appear as the infrastructure develops. Some sectors already have an autonomous capability, while others are yet to see that.

Infotainment is a relatively mature technology, with many content providers and vehicle manufacturers delivering sophisticated services in modern vehicles.

The use of telematics to provide substantial improvements in performance, reliability, and safety has been a minor revolution for the car industry. Using connectivity for continuous vehicle monitoring will improve the reliability and cost of ownership of vehicles by early diagnosis of problems. In the airline industry, there is an increasing focus on the need for continuous connectivity for aircraft telemetry and we are already seeing remote control piloting of drones. It’s important for safety in the vehicle and on the ground that these services are robust, cannot be interfered with, and that access is controlled. Demonstrations such as the highway takeover of a Jeep underline the need for more robust cybersecurity in telematics.

The common use of autonomous vehicles is expected to be just a few years away. While some initial deployment of autonomous buses has taken place, it is likely that the first major sector to launch driverless vehicles will be the taxi industry, with companies like Waymo, Uber, Lyft and DiDi already investing heavily in development of the technology and trials running in a number of countries including the US, Singapore, and the UK. The opportunity exists for taxi services to take over a substantial portion of the trillion dollar personal new and used car market. Key to this vertical is the perceived safety and reliability of driverless cars. Mining has been a leader in the use of autonomous vehicles to replace drivers in high-risk operational situations. While trucks have advanced driverless capability, we’re yet to see driverless fleets.

V2X services provide the interface between the vehicle and the infrastructure domains (V2I), with other vehicles (V2V), and with people (V2P). Some countries have mandated that the capability for remote vehicle control in police pursuit situations be designed into new cars, and accident detection and signalling enables a much more rapid emergency response. We are already seeing proximity keys which can unlock and activate cars, and there are many more capabilities waiting to be developed. Braking system transmitters can automatically inform a following car that braking has commenced, reducing the human reaction time and avoiding crashes. Cars communicating with road signs and traffic lights can help improve traffic flow.

2.6 e-Payment

Smart transport e-Payments is an extension of the financial services e-Payment systems, extended to payments via the vehicle subsystems. Smart cars will not only have automatic servicing, parking and fuel payments, but may also interact with registration and insurance services. This extends the requirement for some of the rigorous financial sector cybersecurity controls into the smart transport solutions.

2.7 Data

While not a subdomain in its own right, data is needed to support the entire smart transportation domain. A foundation of infrastructure and network data will be required, with vehicle to infrastructure connectivity to support dynamic routing. Smart transportation will require a great deal of real time data to be collected, stored and managed with accuracy and responsiveness. This data will need to be secured in line with privacy demands.

2.8 Safety and Security

The term cyber/physical system is sometimes used interoperably with smart systems. It brings a sense of integration of computation, networking, and physical processes. Embedded computers and networks monitor and control the physical processes, with feedback loops where physical processes affect computations and vice versa. In NIST terminology, a cyber/physical system is a co-engineered interacting network of physical and computational components[12]. In Industry 4.0 terminology, cyber/physical systems are enabling technologies which bring the virtual and physical worlds together to create a truly networked world in which intelligent objects communicate and interact with each other[13].

Cyber security and physical safety are no longer separate concerns. When attackers can affect the physical operation of a smart transportation system, network cyber security and physical safety become interdependent. Safety isn't the same as security – but safety can perhaps be considered a subset of security in the cyber/physical world[14].

Ensuring effective cyber/physical security cuts across all subdomains, ensuring the confidentiality, integrity and availability of data and communications, and controlling access to both physical and digital assets. Effective cyber/physical security is a fundamental prerequisite for ensuring the safety of passengers on public transport networks. This includes the availability of safety systems, rapid response from law enforcement, public communications and information distribution, and a variety of surveillance and sensor systems.

Researchers at the Beijing University of Posts and Telecommunications have provided a security and safety framework for cyber physical systems[15]. Their work uses a foundation of integrity, access authentication and authorisation on physical nodes as well as cyber controls and anti-tampering. Sabaliauskaite and Mathur from the Singapore University of Technology

[12] https://www.nist.gov/el/cyber-physical-systems

[13] http://industrie4.0.gtai.de/INDUSTRIE40/Navigation/EN/Topics/The-internet-of-things/cyber-physical-systems.html

[14] https://wwwf.imperial.ac.uk/blog/security-institute/2017/01/03/the-relationship-between-safety-and-security/

[15] http://ieeexplore.ieee.org/document/7026259/

and Design have published research on alignment of safety and security[16]. Their work addresses the four interdependencies between safety and security: conditional dependencies where security is a condition for safety and vice versa; reinforcement where safety and security countermeasures can strengthen each other; antagonism where safety and security can weaken each other; and independence where there is no interaction between safety and security. Their solution to alignment is to apply a failure-attack countermeasure graph to identify conflicts.

A similar approach has been taken at the Austrian Institute of Technology with EU-sponsored research on safety and security in domains including connected automotive, railway, and land transport. The research includes safety and security co-analysis, co-design, verification and validation, and certification, based on a model of failure mode, vulnerabilities and effect analysis. The method involves decomposition of a system into subsystems and parts. Potential failure and threat modes for each part are identified, and the consequences on a local and system level are determined. Through a semi-quantitative approach, the likelihood for the threat modes is determined. Results then become fully aligned safety motivated security goals.

In the vision of *Smart Transport, Smart Security*, Huawei views safety as an imperative within smart security.

[16] https://pdfs.semanticscholar.org/b71d/394d9449f4263eec117369fca569cda4a6e6.pdf

3 Cyber Threats and the Need for Resilience

3.1 Threats

Rail, sea and air transportation centres move vast amounts of people and freight. Heathrow airport, for example, is estimated to have an average hourly movement of around 12,000 people. Consequently, terrorists for many years have made transport systems and infrastructure their targets. There were over 200 incidents of piracy in 2012, both Madrid and London have suffered terrorist attacks on their rail systems. Safety improvements in both infrastructure and transportation has made such attacks extremely difficult, but with the increasing sophistication of cyber attacks terrorists have another weapon to use. Cyber attacks against real time transportation systems must be a primary long term concern with the impact being both in and outside of the cyber domain. Outside of the terrorist threat, transportation systems are at risk from cyber vandalism, from malicious attacks by disgruntled employees, and through deliberate attacks from hackers, hacktivists, and cyber criminals.

Smart transportation applications, networks, and devices can be targets for cyber attacks. Applications may be at risk from internet-borne attacks or attacks that move laterally through their networks. Some applications will disperse application functions to the network edge or device segments and these will be at higher risk due to their larger footprint. The potential threats to a network include destruction of information, corruption or modification of information, theft, removal or loss of information, disclosure of information, and interruption of services. Smart transport systems may be subject to denial of service or unauthorized access attacks through remote internet-borne attacks, through direct access to infrastructure, or via close range proximity networks. These attacks may target vulnerabilities in control systems, information systems, procedures, and controls. In the device segment, transport technology has tended to operate as a closed system which is fairly simple to manage and has a long life. However, the cyber technology that will be used for smart transportation will be widely connected, complex, and have a rapid cycle of change. This means that sustaining a high level of protection can be quite challenging.

A smart transportation cyber threat taxonomy has been developed by ENISA[17]. There are seven threat categories which include acts of nature, accidents and failures, and also include cyber attack. A successful cyber attack on a smart transport system may threaten safety, disrupt transport services, have a financial and reputational impact on the transport operators, and result in criminal damage. In the transport sector, there is a real risk of injury or death should a significant cyber attack be successful.

There are many difficulties in addressing these threats. While transportation operators understand the physical aspects of safety, they may not have the skills and experience necessary to understand the threat to safety via cyber attack. Investment in cyber security may be deprioritized, and testing for vulnerabilities may not be adequate. The slow phasing out of legacy systems can compromise cyber security, especially where these systems have been tactically interconnected with newer systems.

3.2 Resilience

While technical controls are a necessary part of any digital transport solution, they are on their own insufficient to ensure an appropriate level of resilience against cybersecurity

[17] Cyber Security and Resilience of Intelligent Public Transport, ENISA December 2015

threats. The need for cybersecurity must be part of the culture not only of the solution owner, but of the suppliers and partners involved in delivering and operating the solution. Cybersecurity must exist as an integral part of the thinking and actions of people, it implementation must be integrated into processes, and then the controls in the technology will be effective. Particularly in the smart transport sector, cybersecurity must be supported with an appropriate level of physical security.

In 2016, Huawei suggested that it's time for real progress in addressing supply chain risks[18]. Organisations and customers need to the able to take advantage of the full benefits of communications and information technologies that flow from a truly global supply chain. Products and services need to be there when needed, with a product lifecycle approach that minimizes the risk that products will be tainted by malicious actors, or that components may be counterfeit and exploited for malicious purposes. Developing a resilient smart transport system requires attention to cyber security across people, process and technology. Huawei has provided a powerful tool for achieving supply chain security – the 100 requirements of vendors that are needed to achieve end-to-end cybersecurity[19].

People. Staff training and awareness of cyber threats is a good start point, but real resilience means having a strategy for building cybersecurity into everything the organization does, building it into the organizational DNA. Cybersecurity awareness must evolve to cybersecurity understanding, from the top and throughout the organisation.

Process. To be successful, cybersecurity considerations must be included in all processes in the organization, starting with strategy and planning. Designing cybersecure products and services with no single points of failure is fundamental to achieving resilient processes. The US National Institute of Standards and Technology has released Special Publication SP800-160: Systems Security Engineering which provides a disciplined approach to realizing trustworthy secure systems and provides a resiliency framework. Building in monitoring mechanisms and having early warning processes, with the ability to operate in a hardened minimum level of service when under attack, is key to survivability and ensuring safety. All processes must be designed on the assumption that an attacker may be activating them and build in self checking and protection mechanisms. Risk assessments and crisis plans, regularly exercised, will limit the consequences of a cyber attack and enable rapid recovery.

Technology. Technical controls can be used to prevent cyber attack, and to detect any attacks that might circumvent controls. A strategy of technical control defense in depth can be used to limit the likelihood and the impact of both accidents and deliberate attack. Technical controls include encryption, access control, tamper resistance, firewalls, and intrusion and anomaly detection. A particularly important control is host and network monitoring and security analytics to provide early warning of a potential attack, and early detection when one occurs.

A fundamental assumption of system resiliency is that a sophisticated adversary will penetrate your system. In a large and complex system, there will always be flaws and weaknesses in the technology used, the software, the operational environments, and supply chains that adversaries can exploit. Resiliency is about combating the advanced persistent threat, and being able to continue operating and maintain safety even when an adversary has established a presence in the network, even if this means sacrificing some functionality.

[18] The Global Cyber Security Challenge, Huawei Technologies, 2016

[19] Cyber Security Perspectives, Huawei Technologies, 2014

3.3 Changing the perception of technology security

In today's world, the internet provides the interconnectivity for many things, from home automation and appliances to wearable technology and bio-implants. It provides the machine to machine communications between computers and billions of devices. The mobile revolution saw the number of end-point devices exceed one billion in 2002, and the majority of these devices are now online and talking to each other to achieve an increasingly sophisticated level of automated outcomes through what has become known as the Internet of Things (IoT). The complexity and pace of change in the machine-to-machine space and the increasing connectivity between the physical world and the electronic world that it brings is a challenge which requires an integrated systems approach to be taken across what has traditionally been a siloed set of service solutions.

With IoT, it is no longer sufficient to deploy a single device or system. IoT needs to be architected at a business level to coherently deliver the increasingly sophisticated solutions to real world business problems spanning the full cyber-physical spectrum. Similarly, it is no longer sufficient to address security of an IoT device at the component level when it is part of a more sophisticated system. This need to take a systemic view is highly relevant to the area of intelligent transport systems.

The scale and the way in which IoT is changing what we currently perceive of as the internet, and is bringing with it a need to change how we look at technology security.

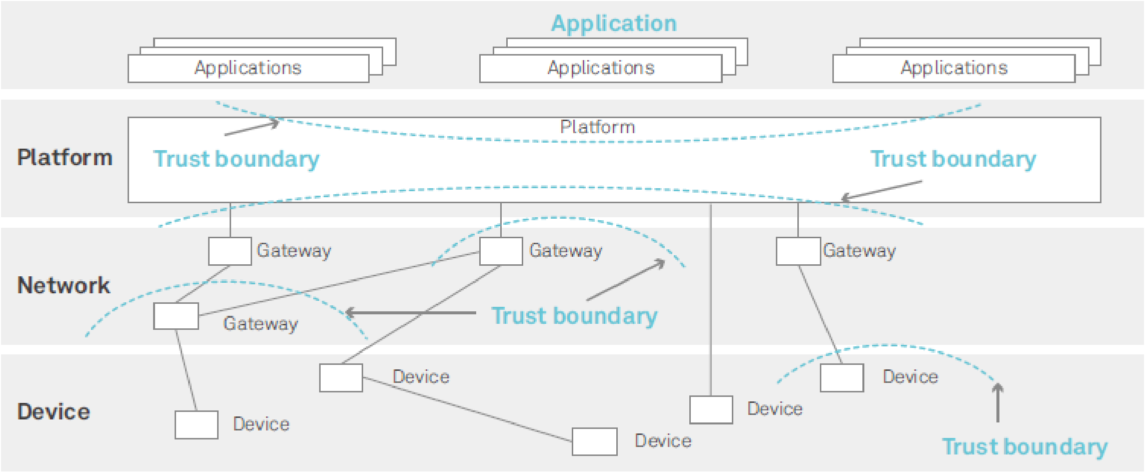
3.4 Huawei's insights into IoT security

Huawei has carried out a detailed study of the problem of IoT security[20]. It notes the high risk profile of embedded IoT subsystems with limited resources, in remote and hard to reach areas. The fact that these subsystems have to cater for a wide variety of higher level uses and deployment scenarios is counter to best practice security, and so another risk factor. It also concludes that there are four key capabilities required to deliver effective IoT security: configurable device defence, malicious device detection and isolation, platform and data protection, and secure operations and management.

One of the key outcomes from consideration of the IoT security challenges is the need for mutual authentication, ensuring devices authenticate each other as well as authenticating to downstream central systems. The scale of attack is another factor which requires a novel perspective on IoT security, where thousands if not millions of devices can be subverted automatically, and networks of devices which can pass on infections across the network and up to the overarching applications. It requires much more focus on trust boundaries than is the case with traditional information technology systems and isolated operational technology systems. Figure 3 depicts the different boundaries of trust.

Figure 3: Domains and Trust Boundaries in IoT.

[20] Huawei IoT Security White Paper 2017



An IoT system can be considered as a layered technology with device, network, platform and application layers, each separated from each other by trust boundaries which reflect the differing risk levels in those domains. With this perspective, end-to-end security across an IoT system can take into account the different trust levels at each layer.

Another consideration for IoT security is that data is not single-purpose, and it needs to be secured in a way that protects it from unauthorised use but makes it available for multiple authorised uses. In addition, not only the data content but its metadata, such as the location it was collected, may need to be protected.

IoT-related security events have shown the sheer scale of IoT can be leveraged maliciously to achieve cyber attack at scale. That means an IoT system of many millions of end points can be brought to bear in a distributed denial of service, or that one newly discovered vulnerability can affect millions of internet end points. Dealing with scale requires a change to traditional defensive security practices.

4 Cyber Security Standards

4.1 Security standards, frameworks, and controls

Many organizations struggle with how to assess the risk their organization faces, and how to chart a path towards a more informed stance on risk tailored to their individual situation particularly in the face of numerous sets of standards and best practices. Many of the traditionally adopted standards and best practices focus on internal controls and are process rather than operationally focused.

In recent times, both the US and the UK have released standards more focused on cyber attack than internal controls, and these are more suited to developing smart security solutions. The US National Institute of Standards and Technology (NIST) has published the NIST Cybersecurity Framework, a set of standards and best practices focused on preventing, detecting and responding to cyber threats. The UK Government issued the Cyber Essentials scheme, which recommended a set of five technical control themes to defend against cyber attack, together with an assurance framework (further detailed in section 5.2).

There are some references for security in the Intelligent Transport sector. ETSI has published a set of Intelligent Transport Systems standards[21] which provide a view of security covering the security architecture and the trust, privacy, access control and confidentiality system requirements.

The Radio Technical Commission for Aeronautics has published the DO-326A - Airworthiness Security Process Specification, which addresses concerns relating to the threat of intentional unauthorized electronic interaction to aircraft safety through data requirements and compliance objectives for aircraft development and certification. This is a core document for ensuring the Aeronautical Information System Security (AISS) of airborne systems.

The international standards community is starting to address the vulnerabilities of vehicle telematics with development of a new standard ISO/SAE 24134: Road Vehicles – Cybersecurity Engineering, which is expected to offer similar guidance to that in the NIST SP800-160 Systems Security Engineering. Independently, the SAE Joint Committee in 2016 published SAE J3061[22] publication Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. This is based on the ISO 26262 Functional Safety process framework and provides recommendations for designing cybersecurity into vehicle systems and covers product design, validation, deployment and communications. It aligns safety hazard analysis with cybersecurity threat and risk assessment, and aligns functional safety requirements with cybersecurity requirements to ensure that cybersecurity supports safety objectives. Some advanced development techniques such as eSafety Vehicle Intrusion-protected Applications (EVITA), Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE), and Healing Vulnerabilities to Enhance Software Security and Safety (HEAVENS) are addressed in the recommended development approach.

The UK Department for Transport has issued the publication Rail Cyber Security Guidance[23]. While this is focused on the digital rail sector, the UK Government is encouraging the wider UK critical infrastructure sector to adopt it. This guidance brings together the NIST Cybersecurity Framework and the UK Cyber Essentials scheme, offering a set of principles

[21] ETSI TS102 940 ITS Security Architecture (and supporting standards ETS TS 102 941, 942, 943)

[22] http://standards.sae.org/wip/j3061/

[23] Rail Cyber Security: Guidance to Industry, Department for Transport, February 2016

and guidance on designed-in security, cyber attack protection, and incident management. More recently, in October 2017, the Australian Rail Industry Safety and Standards Board released a draft version of the Australian Standard (AS) 7770: Rail Cyber Security[24]. This also focuses on the NIST Cybersecurity Framework, and identifies an enterprise security approach be taken to ensure that IoT security is architected to support the business outcomes. It suggests five high level principles for ensuring security: if it's not secure it's not safe; proportionate controls; goal-based security; designed-in security; and defence in depth.

The shipping industry has also worked together to provide guidance on maritime cybersecurity. Sixteen shipping organisations have developed the publication Cybersecurity onboard Ships. This publication applies the NIST framework to the information and operational technology systems onboard ships, including ship-to-shore communications. It covers the complete information security management system scope from awareness to technical controls across cargo management, bridge systems, propulsion, steering, power, onboard security systems, management systems, public networks, and communications.

While focusing on general cyber protection rather than internal control is a good first step, security solutions for the smart transport sector need a dedicated cyber security approach fit for purpose in the transport sector. Smart transport is more than an IT system subject to network attack. A smart transport solution requires an integrated set of high reliability IoT technologies communicating in a private or public networking environment. It needs to have a security paradigm which fuses IoT technologies with cyber protection, applied end-to-end across carrier grade LTE or NB-IoT networks and, in the future, 5G network slices to deliver a demonstrably cyber/physical secure and safe solution.

A comprehensive transport sector architecture will certainly include end-to-end smart transport services in which devices connect to the infrastructure via a proximity network and then connect through backhaul to the core. However, it will also need to consider deployments which support devices operating purely at the network edge, and with the move to 5G slices the additional attack surfaces due to the use of virtualized functions and the orchestration layer.

The Industrial Internet Consortium in 2016 published its security framework for the internet of things[25]. The frame work considers a number of cross cutting concerns which are relevant to all things on the internet, covering aspects of reliability, security, privacy, safety and resilience which together form the trustworthiness of the system. The framework is a foundation and can be applied to any IoT sector vertical.

4.2 Cyber Essentials

The UK Cyber Essentials scheme identifies five technical controls which are required to ensure a baseline of cyber security.

Firewalls and Internet Gateways. Establish boundary and host-based firewalls to restrict inbound and outbound network traffic to a pre-defined set of sources and services, using firewall rules.

[24] Rail Cyber Security, Rail Industry Safety and Standards Board, October 2017

[25] http://www.iiconsortium.org/IISF.htm

Secure Configuration. Ensure that computers and network devices are properly configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

User Access Control. Ensure user accounts are assigned to authorised individuals only, and limit access to only those applications and systems necessary for the user to perform their role.

Malware Protection. Restrict execution of known malware and untrusted software, to prevent harmful code from causing damage or accessing sensitive data.

Patch Management. Ensure that devices and software are not vulnerable to known security issues for which fixes are available.

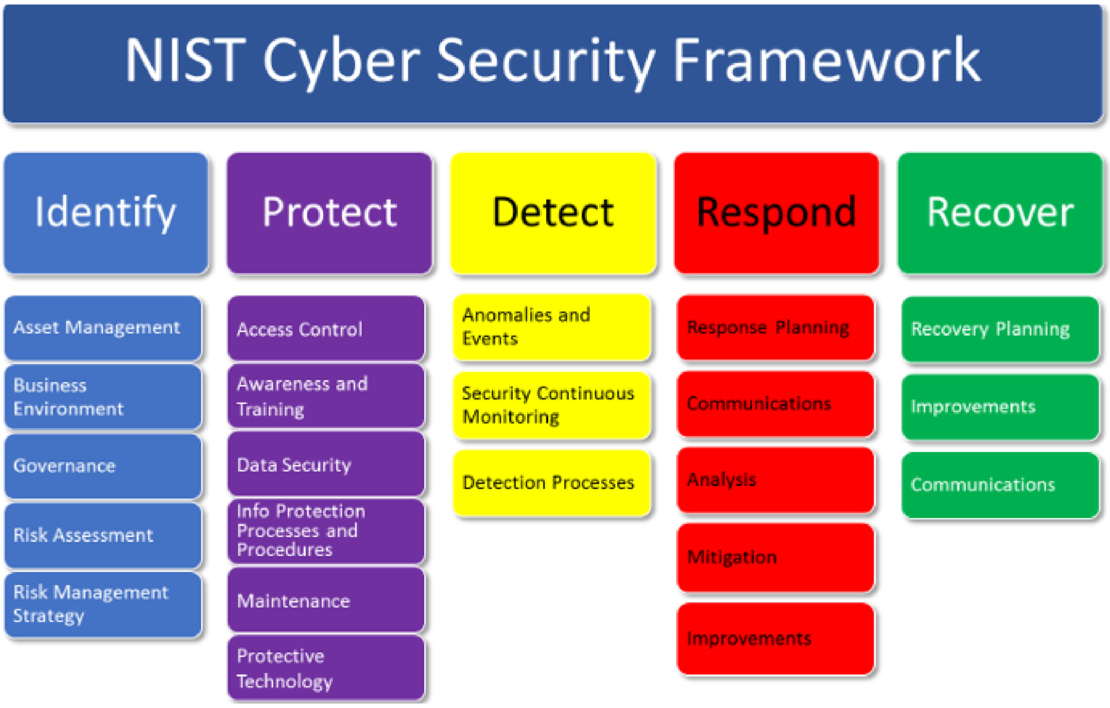
These technical controls can be used to further refine and prioritize investment and effort in the overall cybersecurity control strategy.

4.3 NIST Cybersecurity Framework

The NIST Cybersecurity Framework is designed to help organizations manage cybersecurity risks and to guide cyber security activities in the business, ensuring cybersecurity risks are integrated into the organization's risk management processes.

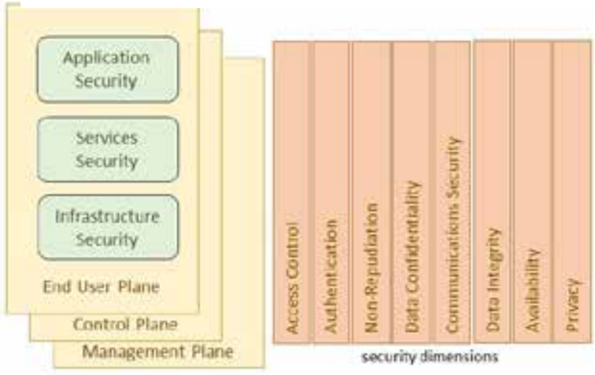
The Framework provides a set of 23 control objectives which are categorized in five groups: Identify, Protect, Detect, Respond, and Recover. The control objectives provide a high level outcome such as Protect: Data Security. These high level outcomes are broken down into individual controls. The NIST Framework doesn't define the detail of its controls, but refers to the control definitions in ISO 27002, NIST SP800-53, CobIT, ASA, CCS, and a number of other pre-existing standards. The NIST Cybersecurity Framework will be an important element of any smart security solution for transportation.

Figure 5: The NIST Cybersecurity Framework



4.4 ITU X.805

Figure 6: ITU X.805 Security Model



ITU X.805 describes a telecommunications security architecture based around the management, control, and user planes, within each of which exists applications, services, and infrastructure. There are then eight security dimensions which apply variously across the model.

The management security plane is concerned with the protection of the operations support administrative, maintenance and provisioning functions of the network elements, including transmission facilities, back-office systems and data centres as well as the fault, capacity, and security functions. The control security plane is concerned with signalling and machine-to-machine communications such as dynamic network routing. The end-user security plane provides security for customer data.

4.5 ETSI NFV-SEC003 Network Function Virtualization (NFV) Security

The adoption rate and interest in network function virtualization is huge amongst mobile operators around the world. The introduction of hypervisors into the technology stack and the use of private clouds to deliver network elements mean that new security challenges have to be addressed. The adoption of NFV will accelerate as 5G starts to deploy.

ETSI has released security guidance on network function virtualization as publication NFV-SEC003. Security in NFV is similar to security in a hypervisor virtualization environment, with cloud based orchestration introducing additional security demands. The standard introduces a baseline of NFV security together with optional capabilities to enhance security where the risks justifies doing so. It also highlights areas where security technologies and practices differ from non-NFV environments. A virtual network function (VNF) may need to perform a variety of different actions and functions which have a security element, of which the most obvious are identity checking and data encryption/decryption. The standard security tools required to perform them rely on the secure provision of a private asymmetric key and associated public key to a specific architectural component. A private asymmetric key (with associated public key), and a trust relationship with a Certificate Authority (CA), can act as the primitives to enable all of other actions and functions. Consequently, the Certificate Authority (CA) is considered a key service within any given NFV context.

NFV introduces the concept of an infrastructure domain which provides a pool of virtual resources such as compute, networking and storage, and a tenant domain which consumes resources from one or more Infrastructure Domains using an orchestration capability to combine virtual infrastructure resources into VNFs and to operate the associated end-to-end network services.

4.6 ITU X.SDNSec

Security is becoming an important issue for software defined networks as carriers look for ways to improve profitability and reduce costs. This again will accelerate as 5G starts to deploy, with SDN being a key enabling technology for a fully 5G deployment.

There is as yet no guidance on security services to protect SDN although some research has been carried out on SDN in smart grids[26]. However, work is currently progressing in ITU SG17 on the development of guidance for delivering security services through SDN and draft Recommendation ITU-T X.sdnsec-1 has been released. This provides a high level architecture to support SDN-based security services and provides a number of example use cases such as firewalls and honeypots. SDNSec security policies are set through the SDN Application Layer to the SDN Controller, which generates new flow entries to set the access control policy rules and deploy them to devices in the Resource Layer. These entries then update flow tables and the new policies can be executed.

For a carrier, the three key criteria for a successful SDN deployment are reliability, security, and resilience. With an increasing focus on delivering services to safety-critical solutions, the telecommunications service will need to operate under faults, misconfigurations, and failures. It will need to be resilient in the presence of malicious attacks and ensure the security of data and services.

Huawei has developed a Carrier Grade agile SDN security solution based around OpenFlow which supports a variety of SDN deployments, including Cloud Data Centre and WAN. The Agile SDN Controller solution implements flexible orchestration and automated security service provisioning for tenants, with up to 12 types of virtualized security capabilities available. The security service provisioning process requires no manual intervention and saves 90% of the manual configuration workload, enabling security services to be provisioned in a matter of minutes and operated in a unified manner. This provides timely protection for resources used by tenants to keep pace with quick service development in virtualized environments. A key feature of this solution is its intelligent awareness function that enables security policies of tenants to migrate with services in real time. The Agile SDN Controller can be used to implement unified visual operations and maintenance (O&M). This improves service management efficiency. It filters service traffic at the network boundary, tenant, and VM levels to provide triple protection. Tenants can collect and analyze logs, files, and traffic in virtualized environments using the cybersecurity intelligence system (CIS), an intelligent Big Data analytics platform. This platform detects abnormal network behaviors with an accuracy of more than 99%, overcoming traditional threat detection tools' problem of low efficiency against upgraded threats.

4.7 ETSI TR 102 940 ITS security architecture

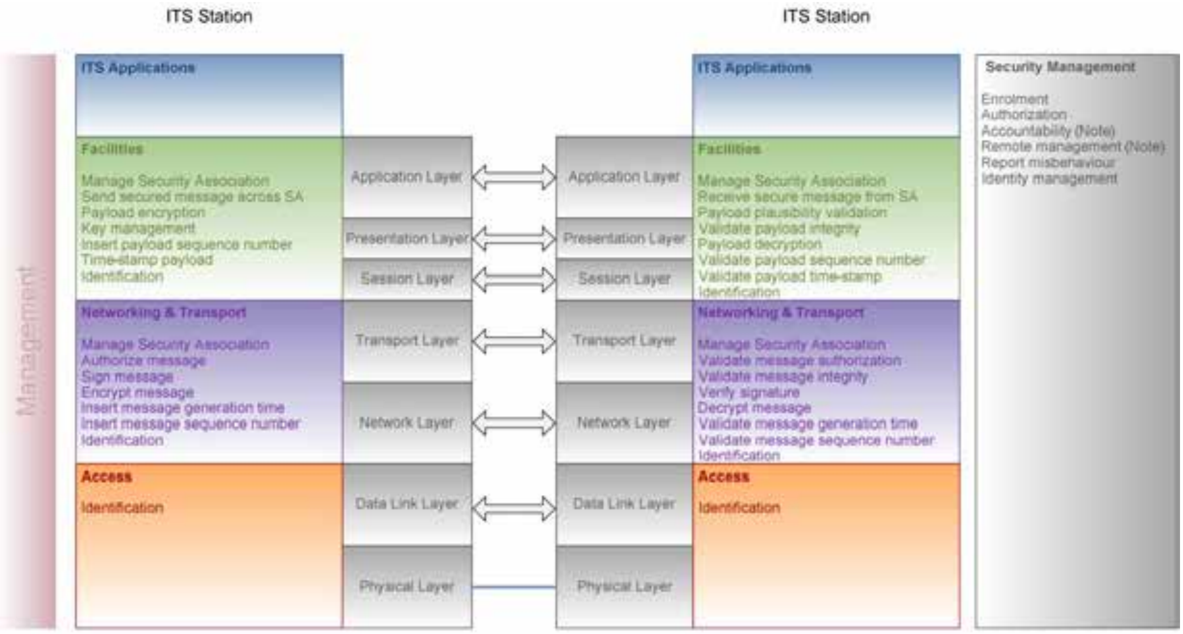
In general, a security architecture is developed by considering the security requirements of the outcomes of the relevant initiative or business. An architecture to support a personal transport smart car will focus on different attributes to that of a digital rail solution or an international maritime freight solution. There may be common attributes, but in essence the security architecture will need to support a specific business-related set of outcomes.

A reference architecture is a generic form of architecture which can be used to hold a common set of architectural elements from which a specific architecture can be created through selection and customisation. This is generally a logical view of security services rather than a physical view of IT components.

[26] A Security Framework for SDN-enabled Smart Power Grids. Ghosh et al, 17th International Conference on Distributed Computing Systems

The European Telecommunications Standards Institute (ETSI) has produced a security reference architecture[27] for an intelligent transport system which defines four layers: ITS application, Facilities, Networking & Transport, and Access. The scope of the architecture supports a range of European projects, and is smart vehicle centric. The guidelines identify the roles and locations of a range of security services to protect transmitted information and manage essential security parameters. These include identifier and certificate management, PKI processes and interfaces as well as basic policies and guidelines for trust establishment. Specifically, the application layer covers driving assistance in the areas of cooperative awareness and road hazard warning; cooperative speed management and navigation; location based services; community services; IT station life cycle management; and transport related financial payment services.

Figure 7: ETSI Security Reference Architecture



The reference architecture provides for three security services applied to applications: authentication and authorization; privacy; and confidentiality. For communications security, it suggests: security association management; single message services; integrity services; replay protection; and plausibility (input checking) validation. Security management is also served with enrolment, authorization, accountability, remote management, misbehavior reporting, and identity management services. These are shown in Figure 7.

This reference architecture can be used to inform the development of specific case security architecture in the smart transport sector.

4.8 Security evaluation specifications

The Common Criteria scheme[28] for security evaluations is a well-recognised and respected approach to establishing the assurance of a product or system through a formal review and

[27] ETSI TS 102 940 ITS Communications Security Architecture and Security Management

[28] https://www.commoncriteriaportal.org/

testing process. It is a national level scheme endorsed by governments, and common criteria evaluations are undertaken in seventeen countries and accepted by a further eleven.

Common criteria can be applied to any product by defining an appropriate set of functionality claims, and evaluating the claims to a pre-defined level of assurance. This approach has been extended to a standard set of functional capability through the use of collaborative Common Criteria Protect Profiles. An example is the collaborative Protection Profile for Network Devices, or NDcPP. This is a common benchmark to use for certification testing of network devices within the Common Criteria scheme to verify their ability to meet a commonly agreed security baseline of protection against relevant threats. This approach removes much of the subjectivity seen in assurance testing against vendor specific security functionality.

There are currently no use case protection profiles for smart transport, but these are likely to emerge as the demand for safety drives government regulations on the transport infrastructure and smart cities.

5 Case Study: Digital Rail

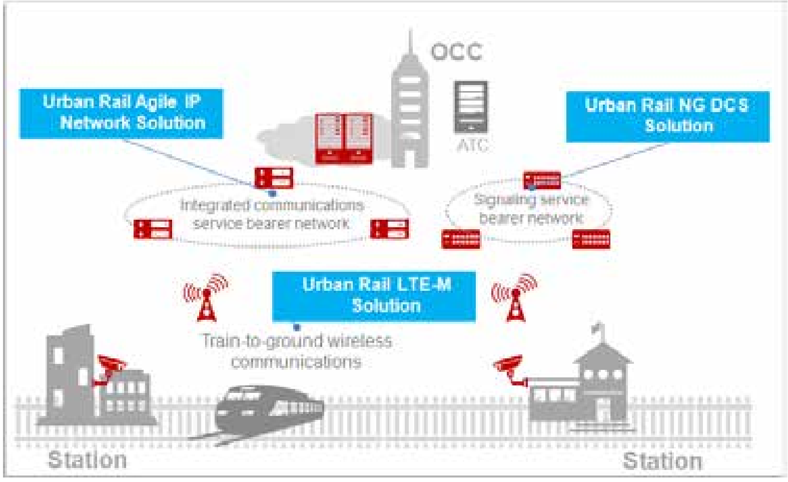
5.1 Developing a smart transport security approach

The requirements for developing a smart security services to support next generation smart transport solutions have been developed in the various standards bodies, but need to be combined in a way which suits specific cases of smart transport. Current accepted practice in cybersecurity is to plan for a certain number of attacks being successful, and taking a risk based approach to controls. For safety critical solutions in the smart transport sector, there needs to be much more emphasis on prevention of, and survivability when subjected to, cyber attack. To see how this can be done, we'll look at how a smart security solution can be developed for one such case, that of urban digital rail.

5.2 Conceptual solution

An urban digital rail solution is typically provided using LTE wireless technologies and all-IP bearer networks to allow multiple services such as communications, train control, dispatching, PIS, and video surveillance to be carried over one network, thereby improving the utilization of network resources, ensuring safe urban rail operations, and generating greater revenues. The use of sensors for predictive maintenance and early warning reduces out of service time and provides a substantial improvement in maintenance costs. The overall concept is shown in Figure 8.

Figure 8: Urban Digital Rail Solution


OCC
ATC
Urban Rail Agile IP Network Solution
Urban Rail NG DCS Solution
Integrated communications service bearer network
Signaling service bearer network
Urban Rail LTE-M Solution
Train-to-ground wireless communications
Station
Station

The signalling system is an integral part of urban rail dispatching, commanding, and security control. Wireless networks allow reliable, uninterrupted, and bidirectional communication between signalling devices on the ground and on-board, and demand reliability, maintenance convenience, bandwidth, timeliness, and security.

5.3 Addressing the cyber threats

The Huawei IoT Security White Paper identifies five major threats to IoT: corruption of systems integrity; system intrusion; malicious privilege abuse; compromise of data security; and service interruption caused by network service attack. X.805, which predates IoT, defines the five threats to networks as destruction of information and/or other resources; corruption or modification of information; theft, removal or loss of information and/or other resources; disclosure of information; interruption of services. In the context of an LTE-based smart rail system, we may want to also consider the threats identified in the NIST Special Publication 800-187: Guide to LTE Security.

For a coherent threat risk assessment we need to consider the action that might be taken by a malicious actor which could result in an adverse outcome. For the risk assessment, we need to assess the likelihood of this and the impact that outcome may have. The threats noted above are outcomes that can occur as a result of specific actions such as network intrusion and malware infiltration. The outcomes then help define the impact and ultimately the risk.

The start point for a smart transport security architecture, then, is to establish a threat matrix as in Figure 9 which identifies the threats across the X.805 device, network and applications layers, as well as considering specifically the OSS and business processes. The threat actors in this context can be considered at a high level to be people inside the organisation and those external to it. The threats then cover the full scope of the cyber-physical digital rail dimension. For convenience, we have included the physical dimension attacks together with environmental problems such as natural disasters, loss of power etc.

Figure 9: Smart Transport Threat Matrix

	Applications	Networks	Devices	OSS	Processes
Environment/ Physical	Data Centre outage	Site outage Physical attack on sites Air segment jamming Eavesdropping on the air segment	Device eavesdropping Device loss/theft	Data Centre outage	
People (insider)	Intrusion from corporate network into applications Local privilege escalation Denial of application service	Malware remote attack on IP backhaul Denial of network service Corporate intrusion into IP backhaul O&M direct access to network elements	Unauthorised use Download of malicious apps to devices Deliberate leaking of information	Unauthorised use Accidental mis-command Malicious mis-command	Non-compliance
People (external)	Remote intrusion into applications Denial of application service	Malware attack on IP backhaul Remote intrusion into IP backhaul O&M direct access to network elements	Malware remote attack on devices Rogues base station acquire device Exposure of K		

Threats help define the set of possible risks to a system, but many of these are addressed by the design of the system components. This is especially the case in mature technologies such as 3GPP mobile networks. The baseline protection in the 3GPP standards for an LTE deployment is robust and sufficient against intense cyber attacks, if properly implemented.

A critical part of this architecture is the IP network. Current networks tend to have strong perimeter defences but are soft once an attacker gains a foothold inside the perimeter. Huawei is developing the next generation of network security which incorporates advanced attack detection and network resilience capabilities in order to defeat sophisticated cyber attack at all points within the network to provide defence in depth. For current generation networks, these capabilities need to be designed in the deployed solution.

A device may be compromised by physical access, through the supply chain, or through a weakness in its own operational protection. A compromised device could allow an attacker to send in malicious traffic through an authenticated connection and gain access to deeper areas of the system. While we can develop robust defences for high performance end points, this is likely to be more difficult when dealing with low power sensor devices. The new low-overhead algorithms and protocols being developed for IoT are addressing this issue.

An open port on the gateway could allow access into the gateway equipment and enable attacks to be directly launched into the core and application. Conversely, attacks on the central processing facilities could lead to an attack coming from the application or core out to the end point. An attacker could gain access to the base unit and inject traffic directly into the IP channel inside the VPN tunnel provided by IPSec. This is an issue which needs to be addressed with a combination of physical security, tamper detection, and electronic security as well as an integrity protocol for the core to ensure that the network edge hasn't been compromised, and increased self-protection at the edge. Protecting against attacks at the outer areas of the network is becoming increasingly relevant as application code migrates to the edge, and gateways take on more device management.

The threat to safety is paramount when considering a smart transport system. The approaches to safety engineering in physical systems may not be as effective in the cyber-physical domain, and new strategies need to be considered which incorporate cyber attack in addition to faults and human failure. There are many vectors through which a cyber attack may occur, and a comprehensive security solution needs to be architected to ensure all these vectors are fully covered.

5.4 Detecting and protecting against cyber attack

The controls required to detect and protect against cyber attack is addressed by the NIST Cybersecurity Framework. There are many controls in the framework and all should all be considered at the network and application level, however there are some which deserve specific mention.

Detect - Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood. This is a key control to apply to the IP backhaul service, looking for anomalies both inbound and outbound that might relate to hacking or malware that has penetrated the solution. Having an isolated anomaly detection system, possible connected using a one way data diode, can provide confidence that it cannot be subverted.

Detect - Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. This is an important control to ensure that the cyber defences are effective and have not suffered degradation through system changes, or a partial penetration.

Detect - Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. The effectiveness of the protection should be tested at regular intervals.

Protect - Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems. In particular, the PR.PT-5 controls provides for systems to operate in pre-defined functional states to achieve availability, and this is the basis of a survivable system. The overall system should have an ability when under attack to continue to operate in a way which ensures safety and removes unnecessary services to reduce the attack surface.

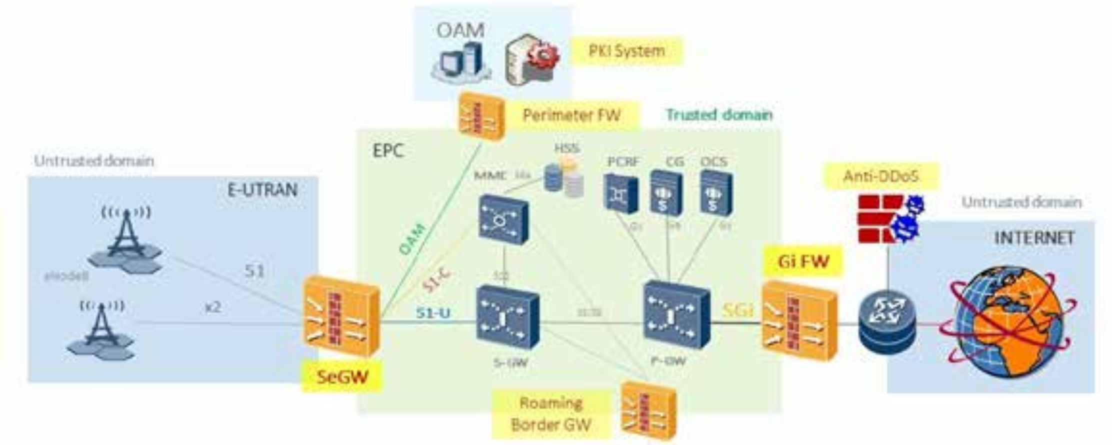
5.5 LTE and backhaul security services

The deployment of an LTE solution provides the basic communications and backhaul security services as part of the communications equipment, based on the management, control and user plane controls for the eight security services defined in X.805. These are designed to protect against eavesdropping, unauthorised access, network device attacks, and attacks on the application and signalling protocols. Management plane security includes management channel security and log/alarm management. Control plane security provides encryption of signalling. Data plane security provides for encryption of data and filtering of viruses and malware.

The LTE radio communications subsystem requires registration of end devices, and authentication prior to accepting traffic. Train-to-ground traffic is encrypted using one of the standard 3GPP LTE algorithms, together with the secure key negotiation service. The main control board provides certificate-based IPSec encrypted communications for backhaul on the integrated communications service bearer network to the operations control centre. The communications solutions establish security associations and can provide integrity services through message checksums and replay protection through message sequencing. End devices will need to incorporate plausibility (input checking) validation to protect against device targeted attacks coming from the upstream infrastructure. The NIST Special Publication 800-187: Guide to LTE Security[29] provides guidance on configuring LTE networks for secure operation. This includes the adoption of physical security controls and setting optional configurations to be secure. The use of network function virtualization is recommended to avoid exposed interfaces between core elements.

While the x2 interface provides eNodeB to eNodeB management functions related to load and interference, comprehensive protection against jamming is an area yet to be addressed by 3GPP.

Figure 10: LTE Security



The radio access domain is untrusted, connecting through backhaul to the trusted core. Within the core the backbone network connects trusted components and incorporates firewalls and security gateways for perimeter defence. An anti-DDOS solution is used to protect the core from internet attacks coming in from enterprise domain connections. These now standard security solutions in LTE ensure only authorized end point devices can communicate and provide reliable and secure voice, text and signalling. Together with device level plausibility validation, this provides a robust and necessary baseline of communications security.

5.6 Application security services

[29] https://csrc.nist.gov/csrc/media/publications/sp/800-187/draft/documents/sp800_187_draft.pdf

Applying the Huawei IoT security approach to the application security services requires attention to platform and data protection for applications, through the use of security services at the application layer. This includes the use of application layer protocols, disk encryption, and integrity protection. These services will typically require PKI and log management and alerting to support them, and authentication services will be needed to enable applications to authenticate devices.

The ETSI security reference architecture provides for authentication and authorization, privacy, and confidentiality at the application level. The radio and IP bearer networks collect and pass data back to the application layer for processing, and so applications need to incorporate plausibility (input checking) validation to protect against attacks coming in from the network. This can be done, for example, using application level cryptography as an over the top service from end point device to application. This can be a powerful strategy for protecting against network based attack.

Application services will be on an internal network which is likely to be, directly or indirectly, connected to the internet. This exposes the application to denial of service attacks, hacking, malware, and leakage of sensitive information. When designing the security of the application systems, it should be assumed that in worst case a malicious attack has penetrated the corporate network and the application server should be hardened. As a minimum, the Cyber Essentials controls should be applied.

5.7 An advanced security architecture to support smart transport

An advanced security architecture for smart transport should take into account the emerging technologies that are being deployed by carriers and enterprises. Software defined network and virtualization across data centres and networks, as well as cloud computing, all play a part in the smart transport architecture of the future. This will become commonplace as 5G services begin to be deployed.

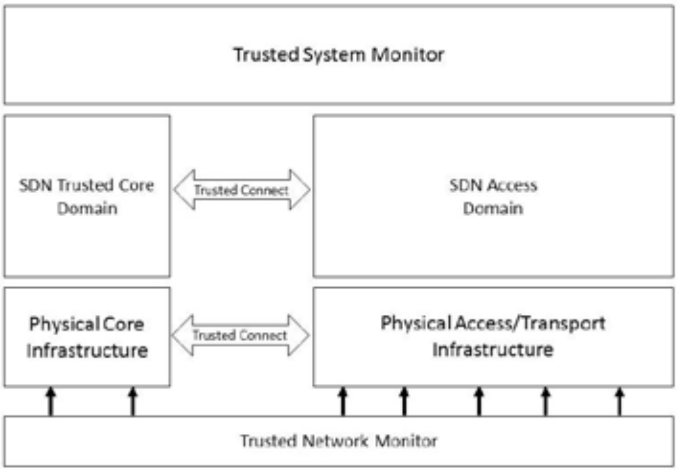
In a smart security solution, there are two key services to consider. The first is a trusted detection mechanism which gets cyber health telemetry from all components. This goes beyond just heartbeats to determine whether the component is alive or dead, but a more sophisticated set of system *vital signs* to ensure there’s no infection. This does not provide a complete security solution as parasitic malware may be hosted and operating in symbiosis with the host component, but it does address the availability of the service. This capability will increasingly become part of the orchestration layer of software defined networks. The second key service is trusted network monitoring, monitoring the traffic flowing along communications paths looking for signs of anomalies or infections. This is becoming more common with big data security analytics tools.

The smart security solution then needs to take account of national sovereignty and defence in depth requirements in the composition of the end-to-end system. A typical approach is to isolate the core from the access and transport (in networking terminology) domain. For an advanced system, this will involve a virtual and a physical layer for each domain.

Figure 11 shows the high level high level security monitoring perspective of a smart security solution. The system monitor exists to enable construction of any software defined components, monitor the health of the system, and recover any damaged components. This has to be a hardened and ultimate trust domain. In the world of software defined networking, this would be the orchestrator layer. By using an extreme trust system monitor, the architecture can provide a high level of integrity checking of other domain components, to deliver very high levels of safety as well as the functional state resilience required for advanced cybersecurity.

The SDN trusted core domain and one or more access and transport domains enable a flexible multi-vendor solution to be deployed which can meet the most rigorous trust requirements. The core exists as a high security zone with a trusted connect from lower security access and transport domains, using firewall or data diode technology. Some of these domains may exist as private cloud instances, such as a CloudRAN domain.

Figure 11: Security Monitoring Perspective



The SDN Trusted Core and the physical core are both high security domains, while the SDN Access and physical access/transport infrastructure can be considered as lower security domains. This is the architecture typically used in current deployments of 4G. The network, or network slice in a 5G context, represented by the SDN and physical infrastructure will contain in-network security across the air link and transmission, and in the elements as required by the network design.

Operational trust can be achieved by having a trusted network monitor able to watch all interactions, develop a normal operating profile, and report on both known attack activity and anomalous activity which should be investigated. This provides the more advanced cybersecurity defences required to detect and trigger response to an attack.

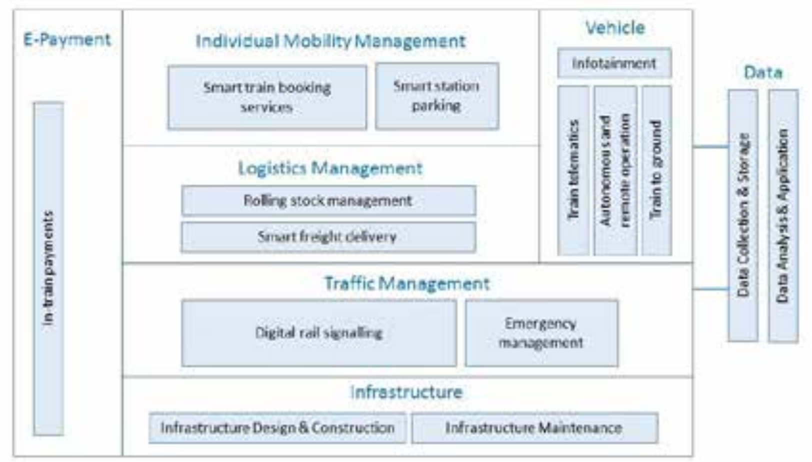
A resilient advanced solution will require essential services to be defined within the overall solution, and have the ability for non-essential services to be stopped in the event of a sustained attack on them. This will avoid depletion of resources and minimise the essential services attack surface.

6 Case Study: Digital Rail

6.1 The smart security architecture for digital rail

The smart transport framework can be applied to the Huawei digital rail architecture as shown in Figure 12. A comprehensive solution designed according to this architecture can provide in-train services such as ePayments and infotainment, and smart solutions for booking train tickets and parking spaces. Rolling stock fleet management and smart freight services can be integrated with train positioning and other transport segments as well as with emergency services in the event of accidents. Digital rail signalling and train telemetry provide significant benefits in the smart train solutions, and autonomous trains will increasingly become the norm. Remote control of trains is a desirable safety feature for both manned and unmanned trains.

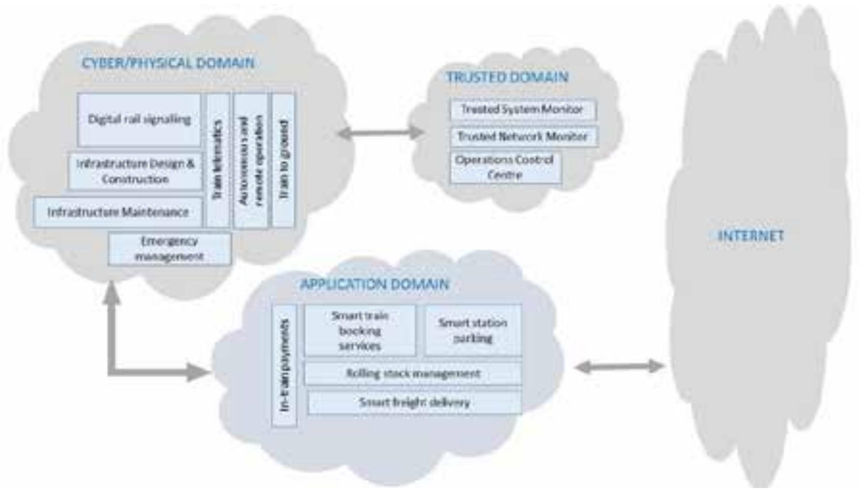
Figure 12: Huawei Digital Rail Architecture



Designing a digital rail solution needs to take into account the relationship between the digital solution and the physical environment, ie it requires a cyber-physical systems approach to support interactions between the train systems and signalling systems, and to have connectivity with ground based sensors in stations and areas in the vicinity of the track. It needs to consider the separation between customer services, corporate interactions, and control systems.

A digital rail system requires high levels of safety which in turn requires a strong cybersecurity solution. Such a system must enforce its security requirements across the cyber-physical boundary, to ensure data can be passed securely between the physical environment, the digital train systems, and the internal application domain. The application domain needs to connect through the internet to external business partners such as other transport segments, financial services, and emergency services. Such connectivity is a source of threats back into the digital train systems and needs to be controlled. Application data will also flow to mobile apps for driver communications and individual mobility. The application domain will incorporate infotainment and other WiFi services for travellers, extended out to the train, but independent of the cyber-physical services. Interactions between the cyber-physical services and other systems requires smart and secure connectivity which is able to filter out malformed packets and malicious commands. Figure 13 shows the high level viewpoint of security for a digital rail solution.

Figure 13: Digital Rail Smart Security Viewpoint

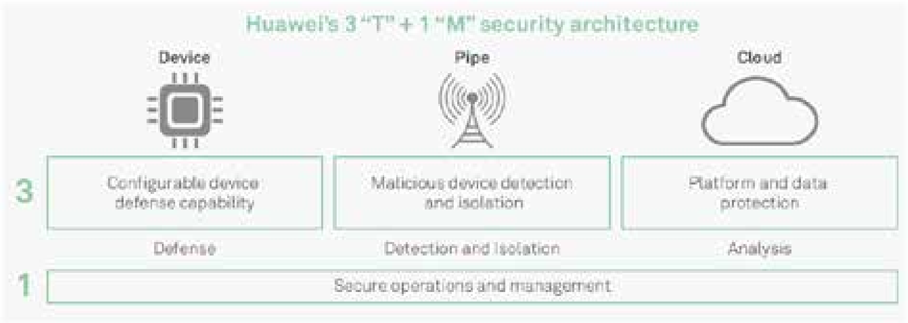


Security is one perspective in an integrated component of the business framework and is managed within an integrated governance regime. The Sherwood Applied Business Security Architecture, SABSA, provides a set of tools and techniques to apply governance across design, development, and ongoing operations. It provides an approach to modelling stakeholder requirements and managing the trust boundaries that are defined in Figure 3.

6.2 Security design considerations

The Huawei IoT Security White Paper identifies four high level capabilities required in an ioT solution as shown in Figure 14, and these can be applied to a digital rail security architecture.

Figure 14: Key IoT Security Capabilities


Huawei's 3 "T" + 1 "M" security architecture
Device
Pipe
Cloud
3
Configurable device defense capability
Malicious device detection and isolation
Platform and data protection
Defense
Detection and Isolation
Analysis
1
Secure operations and management

The first is a configurable device defence capability, and this applies to end point devices such as train driver communications handsets and cab radios, signalling sensors, and so on. The type of security configuration may vary depending upon the resources available in the device, such as authentication and encryption services at the basic level and extending to intrusion prevention and remote security management in more advanced devices. Devices also need to provide secure storage for sensitive material such as encryption keys, and secure boot-up to ensure integrity of the initial operating environment.

The pipe connecting the devices to each other and to the platforms need to be protected, but also can provide a second layer of protection against malicious devices. Pipe protection includes encryption to provide confidentiality, as well as using integrity checks to ensure traffic is received as sent. Secure pipes may also provide replay protection. Malicious device detection and isolation includes identification of malicious packets being sent to application platforms, and rogue devices attempting to connect to radio access points. Protocol identification and filtering also helps detect and isolate rogue systems. Detection of rogue base stations which attempt to maliciously capture in-train radio systems is another capability which should be considered. Access pipes using wireless technology such as LTE will need to be designed to mitigate against jamming.

Traditional cybersecurity techniques are used to protect cloud and on-premise platforms. Perimeter security in the form of firewalls can be used, as well as anomaly detection and intrusion prevention on incoming network interfaces to detect and eradicate malware. Platforms may use plausibility services to ensure that message content is plausible, to help protect against malicious packet attacks. Message security in the form of authentication and decryption services are required to reflect those applied at the device end point. Isolation of data in a cloud hosted solution is important to protect cross attack from other applications on the platform. Application and platform hardening should be applied.

The three sets of technical security capabilities require secure operation and management in order to be effective. This includes identity management to provide enrolment for authorised devices, and log management to provide visibility of operational activities. It also includes routine security tests and evaluations, and security alerting and reporting.

6.3 Security controls

The NIST Cybersecurity Framework has a range of controls to meet these four key areas of security focus. A summary of the application of these controls to the four areas of security is provided Appendix based on an Operator’s perspective of their digital rail eLTE solution.

7 Conclusion

7.1 A smart transport security architecture for the future

The rate of deployment of smart transport solutions is accelerating and is likely to increase exponentially over the next five years as driverless cars appear and quickly become dominant in the transport sector. The standard of security provided in modern communications networks will support smart transport but will be insufficient on its own to meet the demands of safety and reliability that will emerge.

Smart security design will be required to bring together existing approaches to wireless communications security and advanced cybersecurity trust domains into a new security model to support smart transport. The basic building blocks exist with the security work of the ITU, ETSI and NIST. By combining these to meet case-specific requirements, a smart security solution which meets the safety and reliability objectives can be achieved. New security technologies are emerging to meet the advanced cybersecurity threats, and these can be integrated with standard smart transport solutions to substantially improve their security and safety.

7.2 Huawei and smart transportation cybersecurity

Huawei is a leader in architecting and delivering smart transportation solutions and I one of the world's leading providers of eLTE solutions. Already, by applying cybersecurity to every part of its operation, Huawei delivers robust and secure technologies which ensure high performance, high reliability solutions for customers.

With its framework for smart transportation, Huawei has established a common understanding of opportunities for innovation across the sector. Adding the advanced IoT trust domains concepts to the existing security models for wireless networks enables Huawei to deliver safe and secure smart transportation systems using 4G communications, in a way which will enable seamless transition to future 5G technologies.

APPENDIX

NIST Cybersecurity Framework Digital Rail

Id	Description	Device	Pipe	Platform and Data	Operations & Management
ID-AM-1	Physical devices and systems within the organisation are inventoried	An electronic inventory (asset register) is typically provided by the eLTE OSS, incorporating both manual enrolment and automated discovery. This can be augmented with externally input physical asset details. Provide details of the asset register.			
ID-AM-2	Software platforms and applications within the organisation are inventoried				
ID-AM-3	Organisational communication and data flows are mapped		Communications and data flow maps should be included in the design documentation.		
ID-AM-4	External information systems are catalogued			Any corporate, partner, or 3rd party systems which interface to the digital rail system should be described.	
ID-AM-5	Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	Safety critical components should be identified and given priority, followed by network resilience, and then prioritisation based on business value. A business oriented analysis of security, such as provided by the Sherwood Applied Business Security Architecture (SABSA) can be used to formally derive this.			
ID-AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established				A Responsibility, Accountability, Consultancy, and Inform (RACI) chart can be used to describe roles and

					responsibilities.
ID-BE-1	The organisation's role in the supply chain is identified and communicated				All parties (owner, partner, supplier, service provider) should be shown in a supply chain map.
ID-BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated				The industry sector is Transport and the organization's role is an Rail Transport Operator (RTO).
ID-BE-3	Priorities for organizational mission, objectives, and activities are established and communicated				As for ID-AM-5, the priority should be defined with public and staff safety first, followed by network resilience and then business value.
ID-BE-4	Dependencies and critical functions for delivery of critical services are established				A SABSA conceptual analysis can be carried out to determine criticality and dependencies.
ID-BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	A SABSA conceptual analysis will describe the critical services, and will traceably show how the solution is designed with resilience and redundancy in mind. This will cover the end-to-end solution and will evidence that there are no single points of failure.			
ID-GV-1	Organisational information security policy is established				Reference the corporate Information security policy.
ID-GV-2	Information security roles & responsibilities are coordinated and aligned with internal roles and				Roles and responsibilities

	external partners				should be included in the RACI at ID-AM-6, and external partner interfaces should be defined
ID-GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed		Legislative and regulatory requirements should be covered in Information Security policy. The eLTE network introduces additional obligations for spectrum use.		
ID-GV-4	Governance and risk management processes address cybersecurity risks	A cybersecurity risk assessment of the digital rail solution should be carried out and maintained, and risks registered and managed through the life of the digital rail solution.			
ID-RA-1	Asset vulnerabilities are identified and documented	Asset vulnerabilities should be identified and documented during the risk assessment at ID-GV-4.			
ID-RA-2	Cyber threat intelligence and vulnerability information is received from information sharing forums and sources				Threat intelligence should be sourced from public sources, equipment vendors, and/or a commercial threat intelligence service
ID-RA-3	Threats, both internal and external, are identified and documented	The risk assessment at ID-GV-4 should start with a matrix of threat categories, populated with threat models from X.805, the LTE Security Guidance, the RSSB Cyber Security Guide, ENISA, and STRIDE. In addition, real time operational technical threats may be identified through any monitoring systems.			
ID-RA-4	Potential business impacts and likelihoods are identified	The risk assessment will address business impacts for various threats, and this should be further expanded as a result of the SABSA assessment.			
ID-RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	The risk assessment should follow the ISO31000 model which incorporates all these factors, and these will cover devices, pipe, platforms, and management processes.			

ID-RA-6	Risk responses are identified and prioritized				The risk assessment is reported for mitigation purposes in risk prioritized order.
ID-RM-1	Risk management processes are established, managed, and agreed to by organisational stakeholders				The risk management processes follow ISO 31000.
ID-RM-2	Organisational risk tolerance is determined and clearly expressed				The risk assessment should be used to confirm risk tolerance either through accepting or mitigating the identified risks.
ID-RM-3	The organisation's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis				
ID-SC-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organisational stakeholders				The supply chain processes in line with ID-BE-1 should be fully described in a formally approved Supply Chain Security document. Ideally, the business should seek ISO28000 certification.
ID-SC-2	Identify, prioritize and assess suppliers and partners of critical information systems, components and services using a cyber supply chain risk assessment process				3rd Party Security controls should be implemented, including annual self-assessments and 3rd Party audits.
ID-SC-3	Suppliers and partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan.				
ID-SC-4	Suppliers and partners are monitored to confirm that				

	they have satisfied their obligations as required. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted				
ID-SC-5	Response and recovery planning and testing are conducted with critical suppliers/providers				An incident management process should be defined which includes annual crisis exercises including critical suppliers.
PR-AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes				A formal identity provisioning process should be defined.
PR-AC-2	Physical access to assets is managed and protected	Devices will typically operate outside of physical control. Cab radio equipment may have some levels of physical control.	Physical access to buildings and network sites should be in place and managed. Physical access logs should be reviewed.		
PR-AC-3	Remote access is managed				A remote access management process should be defined for all remote access including 3rd level vendor support.
PR-AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties				An access management process should be defined with requests subject to business approval.
PR-AC-5	Network integrity is protected, incorporating network segregation where appropriate		The detailed digital rail solution design Should show the		

			network segregation		
PR-AC-6	Identities are proofed and bound to credentials, and asserted in interactions when appropriate	Userid and password should be requested where appropriate for access to systems.			
PR-AT-1	All users are informed and trained				All users should be provided with cybersecurity training. Engineers should be given product specific vendor security training courses.
PR-AT-2	Privileged users understand roles & responsibilities				Users should formally acknowledge their responsibilities associated with privileged access.
PR-AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities				Supplier obligations should be defined in contracts. Partner obligations should be defined in MoUs.
PR-AT-4	Senior executives understand roles & responsibilities				The RACI at ID-AM-6 should have associated detailed descriptions of responsibilities, and these can be formally briefed to all parties.
PR-AT-5	Physical and information security personnel understand roles & responsibilities				
PR-DS-1	Data-at-rest is protected	Data is at rest should be protected through device encryption, eg hardware backed datastores on smartphones.		Data is at rest it is protected through a combination of encryption and physical security.	

PR-DS-2	Data-in-transit is protected		The 3GPP eLTE specification provides for airlink data protection, and IPSec should be used on the backhaul.		
PR-DS-3	Assets are formally managed throughout removal, transfers, and disposition	Data should be scrubbed from assets prior to disposal and when being return for support.			
PR-DS-4	Adequate capacity to ensure availability is maintained				Operational procedures should include continuous capacity planning.
PR-DS-5	Protections against data leaks are implemented	Devices should be pin-protected.	Network monitoring should be used to detect significant data leakage events.	Workstations should be locked down with no USB access and no internet access.	
PR-DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	Application software on the device should have integrated integrity controls in place.	eLTE and IPSec security includes integrity checks on data	Software should have integrated integrity controls in place, or have file integrity checking tools applied.	
PR-DS-7	The development and testing environment(s) are separate from the production environment				An independent dev/test network should be in place.
PR-DS-8	Integrity checking mechanisms are used to verify hardware integrity	Where possible, hardware integrity checks should be configured.			
PR-IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating appropriate security principles (e.g. concept of least functionality)	All components should be hardened prior to operational acceptance			
PR-IP-2	A System Development Life Cycle to manage systems is				The digital rail

	implemented				solution should be managed through a formal SDLC process.
PR-IP-3	Configuration change control processes are in place		Configuration integrity should be audited		Change management should be enforced on the digital rail solution.
PR-IP-4	Backups of information are conducted, maintained, and tested periodically				A backup regime should be implemented for the digital rail solution and tested quarterly.
PR-Ip-5	Policy and regulations regarding the physical operating environment for organisational assets are met		Physical environment controls should be audited		Policy on physical operating environments should be defined.
PR-IP-6	Data is destroyed according to Policy			Data destruction should be audited	Policy on secure data destruction should be defined.
PR-IP-7	Protection processes are continuously improved				Regular security testing should be carried out to identify weaknesses and mitigations applied through the risk register and remediation programme.
PR-IP-8	Effectiveness of protection technologies is shared with appropriate parties				Security reports may be included in information sharing exchanges.

PR-IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed				Incident response process should be defined and plans developed for specific types of incident.
PR-IP-10	Response and recovery plans are tested				Response plans should be included in cyber crisis exercises
PR-IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)				Staff should be vetted prior to employment and sign cybersecurity obligation statements. Credentials and access should be removed on termination.
PR-IP-12	A vulnerability management plan is developed and implemented				A vulnerability scanning and patching management plan should be defined
PR-MA-1	Maintenance and repair of organisational assets is performed and logged in a timely manner, with approved and controlled tools				Maintenance policy is defined, including sanitization of devices prior to leaving the organization.
PR-MA-2	Remote maintenance of organisational assets is approved, logged, and performed in a manner that prevents unauthorized access				
PR-PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy		Operational logs are transmitted for central monitoring and recording		A log management policy is defined and implemented

PR-PT-2	Removable media is protected and its use restricted according to policy				Removable media should not be enabled
PR-PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	All technology systems will be hardened to remove unnecessary functionality.			
PR-PT-4	Communications and control networks are protected		The airlink has eLTE protection and IPSec is used to protect the backhaul		
PR-PT-5	Systems operate in pre-defined functional states to achieve availability (e.g. under duress, under attack, during recovery, normal operations).				The operating states should be defined and specific attention will be given to any changes required for operating under attack.
DE-AE-1	A baseline of network operations and expected data flows for users and systems is established and managed		Anomaly detection systems can be used to establish network behavior norms and alert on anomalous activity		
DE-AE-2	Detected events are analyzed to understand attack targets and methods		Incidents involving malicious activities on the network or platforms should be analysed		
DE-AE-3	Event data are aggregated and correlated from multiple sources and sensors			A central SIEM capability should be incorporated	
DE-AE-4	Impact of events is determined				The first stage of incident response should be to establish the impact.

DE-AE-5	Incident alert thresholds are established		Anomaly detection thresholds should be defined	The SIEM should be configured with incident alert thresholds.	
DE-CM-1	The network is monitored to detect potential cybersecurity events		Intrusion and anomaly detection should be in place		
DE-CM-2	The physical environment is monitored to detect potential cybersecurity events		CCTV monitoring should be used end-to-end across the external network		
DE-CM-3	Personnel activity is monitored to detect potential cybersecurity events				Physical and logical access should be monitored
DE-CM-4	Malicious code is detected		Intrusion detection should be in place to monitor for malicious payloads in traffic	Anti-virus solutions should be active on all systems	
DE-CM-5	Unauthorized mobile code is detected				
DE-CM-6	External service provider activity is monitored to detect potential cybersecurity events		All external access to the system (eg remote maintenance) should be recorded.		
DE-CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	Connectivity requires an activated SIM and enrolment at the OSS. Airlink monitoring for rogue stations is not required	Network monitoring should be configured to look for unauthorized devices and activity	Regular system audits should be carried out	
DE-CM-8	Vulnerability scans are performed		Vulnerability scanning should be carried out regularly		
DE-DP-1	Roles and responsibilities for detection are well defined to ensure accountability				Roles and responsibilities are included at ID-AM-6

DE-DP-2	Detection activities comply with all applicable requirements				
DE-DP-3	Detection processes are tested		Penetration testing will include validation that known classes of malware and unauthorised activity can be detected		
DE-DP-4	Event detection information is communicated to appropriate parties				Event detection information will be communicated as detailed in the Incident Management policy.
DE-DP-5	Detection processes are continuously improved		Detection processes should be reviewed on a continuous basis and improvements applied to ensure detection techniques keep up with external threats.		
RS-RP-1	Response plan is executed during or after an event		Incident response plans should be activated upon detection of an appropriate incident		
RS-CO-1	Personnel know their roles and order of operations when a response is needed				Staff should be trained in response procedures and an annual incident response exercise should be conducted
RS-CO-2	Events are reported consistent with established criteria				Events will be reported from the SIEM based on configured criteria
RS-CO-3	Information is shared consistent with response plans				Information will be shared to ensure response plans can be executed efficiently and effectively.

RS-CO-4	Coordination with stakeholders occurs consistent with response plans				Coordination and communication with stakeholders will be defined in the response plan. Annual response plan exercises will ensure coordination and communication is tested.
RS-CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness				Cybersecurity event Information may be approved for sharing within information exchange forums.
RS-AN-1	Notifications from detection systems are investigated		Alerts from the intrusion and anomaly detection systems should be triaged and investigated.	SIEM alerts should be investigated.	
RS-AN-2	The impact of the incident is understood	Incident management practices require that the impact of an incident is assessed at the start of incident response and maintained throughout the response process.			
RS-AN-3	Forensics are performed	Where appropriate, internal or external forensics services may be used.			
RS-AN-4	Incidents are categorized consistent with response plans	Incident categorization will follow the agreed corporate IT incident management category scheme. Specific incident types will be aligned with response plans where such plans exist.			
RS-MI-1	Incidents are contained	The incident management process will seek to contain incidents as quickly as possible in order to limit the damage and minimize the recovery effort.			
RS-MI-2	Incidents are mitigated	Incidents response will require recovery of any impaired services, root cause analysis, and mitigation of the root cause.			
RS-MI-3	Newly identified vulnerabilities are mitigated or				New vulnerabilities

	documented as accepted risks				will be assessed and added to the risk register. Treatment priority will be assessed
RS-IM-1	Response plans incorporate lessons learned				The incident management process will include feedback on learnings
RS-IM2	Response strategies are updated				Response strategies will be reviewed annually and updated as appropriate. Where shortcomings are identified during an incident, plans will be updated as part of learnings feedback.
RC-RP-1	Recovery plan is executed during or after an event				The recovery plan will be invoked as defined in the incident management process
RC-IM-1	Recovery plans incorporate lessons learned				Where lessons learned identify improvements to recovery plans, these will be part of incident feedback and be incorporated into the plans
RC-IM-2	Recovery strategies are updated				Recovery strategies will be reviewed annually and updated

					as appropriate. Where shortcomings are identified during an incident, plans will be updated as part of learnings feedback.
RC-CO-1	Public relations are managed				Corporate PR will manage reputation and public relations
RC-CO-2	Reputation after an event is repaired				
RC-CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams				Should an incident occur, the Incident Manager will maintain regular communications with internal stakeholders and management teams.