Developing Cyber Security Asset Management Framework for UK Rail

Shruti Kohli
BCRRE, University of Birmingham
Birmingham, Great Britain
s.kohli@bham.ac.uk

Abstract— **The sophistication and pervasiveness of cyber-attacks are constantly growing, driven partly by technological progress, profitable applications in organized crime and state-sponsored innovation. The modernization of rail control systems has resulted in an increasing reliance on digital technology and increased the potential for security breaches and cyber-attacks. This research paper showcases the need for developing the secure reusable scalable framework for enhancing cyber security of rail assets. A Cybersecurity framework has been proposed that is being developed to detect the tell-tale signs of cyber-attacks against industrial assets. This framework will be based on the concepts of developing protection profiles for railway assets such as point machine and evaluation assurance level in order to certify that chosen railway asset meet required security and safety properties. Endeavor is to make cyber health assessment of railway assets to prevent cyber-attacks.**

Keywords—Rail asset, Cyber Security ,Cyber Ontology, Protection Profile,UK Rail, Rail Security

I. INTRODUCTION

Railway transport plays a major role for international, intercity and suburban connections, requesting a wide and efficient exchange of information with the other transport modes and with the final user. This increased openness and interconnection of the railway systems, brings an even greater need for effective cybersecurity, guarding against malicious threats that could compromise both safety and operational performance. There had been many instances of cyber-attack on cyber-physical system in the past [1]. A cyber-attack reportedly disrupted Israel's network in September. A Trojan horse programme infiltrated the security camera system of the Carmel Tunnels toll road leading to a 20-minute shutdown of the road and an eight-hour shutdown the following day, causing widespread congestion[2]. With increasingly more reliance on web-based security systems, additional threats may occur in the form of denial of service (DoS) attacks[3]. There had been evidence for attack for extortion on control systems in recent past[3]. Although, no concrete evidence has been identified terrorists, activists, and organized criminal have always been the potential threat to control systems[18]. UK rail infrastructure operator Network Rail is in the planning to replace the old, analogue train signals with the European Rail Traffic Management System (ERTMS), a digitalised, more effective system that is rapidly becoming the norm internationally[16]. However, this transition has raised many concerns and has become talk of the town. It is anticipated that this move will leave trains vulnerable to security breaches and cyber attacks, potentially with deadly consequences. Continuous efforts are being made to conduct security audit of ERTMS to identify potential vulnerabilities and suggest mitigations[16]. Table [1] below highlights some of the instances of cyber-attack[19] that have occurred in the past including the attack on rails.

TABLE I. CYBERATTACK INSTANCES

Stuxnet, 2010 [4]: Computer worm discovered in 2010. Targeted Siemens ICS controlling nuclear centrifuge devices. Reportedly destroyed 1/5 of Iran's nuclear centrifuges. Siemens released a detection and removal tool
US Rail Attack, December 2012 [5]: Hackers attacked US Rail Company over 2 days. Rail operations delayed by 15 minutes. Deemed to be a 'random incident' - not a targeted attack on rail
Shamoon, 2012 [6]: Shamoon malware virus infected the business systems of the Saudi Aramco oil company. Although the attack did not directly target critical oil production ICS, it wiped 33,000 – 55,000 workstations at the organisation. An analysis of the virus found that the creators were skilled, but amateurs and that the system had been infected by a disgruntled insider through a USB key. The rail industry should be prepared for attacks on business systems as well as safety-critical ICS.
German steel mill, 2014 [7]: In 2014, it was reported that a steel mill in Germany had suffered "massive" damage when a cyber-attack prevented a blast furnace from shutting down correctly. The attackers had gained access to industrial control systems through a spear-phishing attack on the business network. The attack highlights the danger of presuming that business networks and industrial control systems are not connected, or that an 'air gap' exists between them.

Railway being a critical national infrastructure is vulnerable to attacks from amateur hackers, organised criminals, industrial spies, or disgruntled employees[15]. All of these to one degree or another may have the motivation and an increasing technical capability to exploit vulnerable systems. Network Rail, a leading railway of UK has recognized the risk posed by cyber-attack. Figure [1] represents the multiple sources from where cyber security threat to railway infrastructure may emerge[8].

Fig. 1. Multiple Sources of Cyber Security Threat to Rail Assets

II. Development of Cyber Security Asset Management Tool (CAMT) Framework

National Institutes of Standard Technology (NIST) Cybersecurity Framework [12] is a popular framework used to by industries to secure critical infrastructure. The purpose of the framework is "to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. It is comprised of a Core, a Profile, and Information Tiers. The Core contains standards and best practices that are common across all sectors and industries. The standards are divided into five functions: Identify, Protect, Detect, Respond and Recover, which are generally consistent with industry and international information security standards such as ISO 27001[12]. Although it does not fool proof it provides a starting point to secure industry assets.

In this research work possibility of creating cyber security asset management framework is being explored. The objective is to evolve the cybersecurity standards from a syntactic representation to a more semantic representation. Work is being done in direction of developing a Cyber Asset Management framework that includes following features:

1. Conducting threat analysis to identify the vulnerable point at which rail assets are prone to cyber-attacks.

2. Developing approaches that can leverage existing work taking place in the field of transportation security, encouraging reuse of models and maximizing the benefit of the work.

3. The approach is scalable and can be integrated with many other cyber security ontologies being developed in other areas to counter cyber-attacks on Cyber-physical systems. Existing ontology work developed jointly by the BCRRE team at the University of Birmingham and Siemens Rail Automation resulted in candidate core ontology for the rail domain [13][14]. The scope of the rail core ontology was identified based on proposed implementation areas, perceived cross-application usefulness, and implicit domain knowledge. The figure[2] represents an instance of railway infrastructure that could be modelled using the ontology. The proposed framework includes abstract levels to encapsulate different asset interactions and hence provide guidelines for protecting each rail asset.

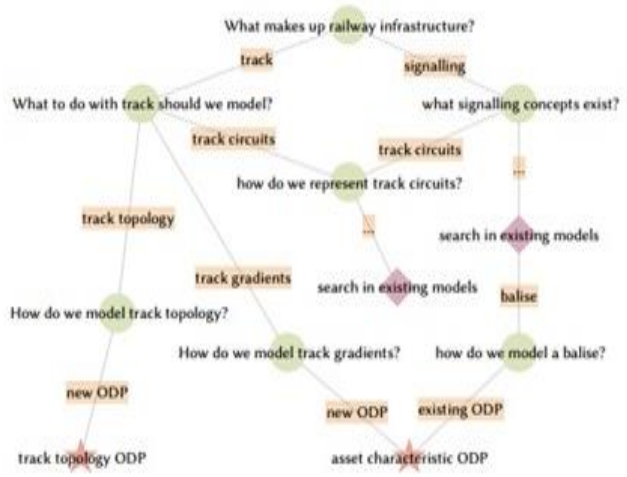

Fig. 2. Representation of Rolling Stock Assets of Railways

The key aims of CAMT can be described as follows:

1. Creation of a Diamond Model of Cyber Rail Assets to measure their vulnerabilities to cyber-attack. The model is required to create cyber situational awareness for protecting sensitive data, monitor fundamental operations, and protect rail assets.

2. Identifying and documenting cyber security standards that define accessibility as well as categorizing the degree of accessibility of rail assets to different rail stakeholder groups. This is tantamount to the creation of protected profiles that could be provided with privileged access to remotely monitor cyber assets;

3. Creation of a modular systems architecture that is scalable and extensible for data volume and variety. Using an RDF triple store and OWL inference, instance data and domain knowledge are transparently delivered to applications, allowing existing applications to be protected from changes to backend data implementations, and easing the development of new software accessing the data resources. Ontologies are being developed for various rail equipment and corresponding data sets. Sensor data, gathered via the IoT can be associated with asset instances in the triple store via in-memory database such as REDIS, buffering the high-throughput data and preventing excessive triggering of reasoning over the ontology instance[20].

4. Improved FMEA (Failure Mode Effect Analysis) of cyber assets through the inclusion of a failure mode type for "cyber failure" that captures the concept of a cyber threat.

This paper represents research in progress. Some of these features have been described in the sub-sections below:

A Creation of a Diamond Model of Cyber Rail Assets

Diamond Rail Asset Model is being created to measure their vulnerabilities to cyber-attack. The vulnerability analysis is conducted for rail assets like Railway Signalling, Point Machines, and Railway tracks. The Diamond model developed by researchers at MITRE[21] has been modified to conduct the feasibility study of Cyber Security. Figure [3] represents the Diamond Model for Rail assets. In its simplest form the model describes that an adversary deploys a capability over some infrastructure against the victim. E.g. Hacktivist manipulates sensor data to disrupt train service impacting the passengers. As done in Diamond model based research before analysis or machine can populate the model vertices as events are discovered and detected[21].

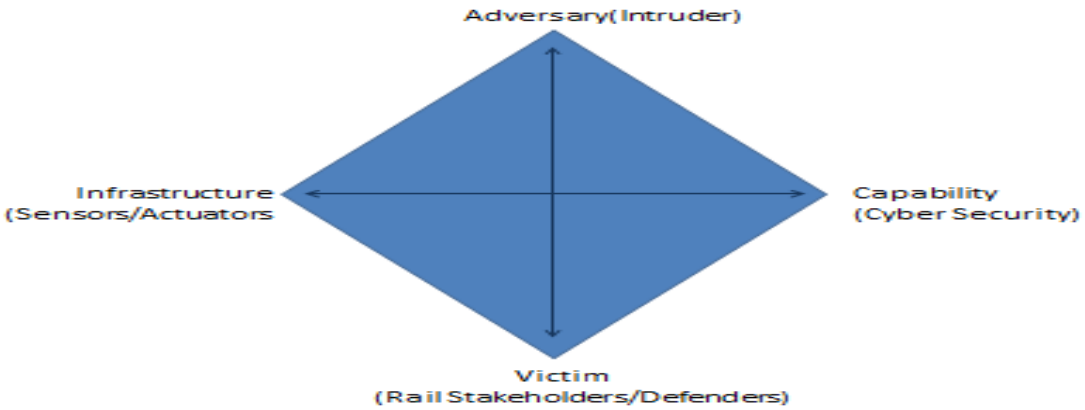

Fig. 3. Diamond Model for Rail Assets

Vertices= {Adversary, Infrastructure, Capability, Victim},

Edges={{Adversary, Capability},{Adversary, Infrastructure}, {Infrastructure, Capability}, {Infrastructure, Victim},{Capability, Victim}}

Events = {(Adversary, $Confidence_{adversary}$),(Infrastructure $Confidence_{infrastructure}$),(Capability,$Confidence_{capability}$), (Victim,$Confidence_{victim}$), ($Timestamp_{Start}$,$Confidence_{Start}$, (Timestamp,$Confidence_{End}$),Other meta features…)

Event could be formally defined as a n-tuple where each element of the tuple is knowledge of a feature combined by independent confidence value. This value needs to be calculated quantitatively or qualitatively by monitoring the conditions that caused event to happen. The edges define the relationships that exist between the various vertices and are important for identifying the events that involve cyber-attack.

Assuming that the key stakeholders are the railways itself and the intruder could be anyone with mal-intentions. Determined tasks are:

1. **Identify the victim asset (targets):** Victim Assets are the attack surface and consist of the set of networks, systems, components, sub-components etc.. which the adversary directs their capabilities. Victim assets often exist both inside and outside a persona's control and visibility but are still available for targeting by an adversary.

2. **Identify the Adversary:** Set of adversaries could be insiders, outsiders, individuals, groups, and organizations) which seek to compromise the running control systems. Various personnel in the rail staff can have limited/unlimited access to rail assets.

3. **Collecting Meta Information:** While identifying cyber attack as an event it is important to collect meta features such as Timestamp, Phase, Result, Direction, Methodology Resources to describe the occurring of a cyber-attack event. Some of the important meta features could be incorporated in following classes:

a. Means: Describes various methods of executing an attack and consists of sub-classes like BufferOverFlow, SynFlood, LogicExploit, Tcp-PortScan etc.. It includes details of observed or potential attacker Tactics, Techniques, and Procedures.
b. Consequences: Used to list possible outcomes of an attack. For possible cyber-attacks, it may take values such as DenialOfService, PrivilegeEscalation.
c. Attack: This class represents cyber threat attack.
d. Attacker: This class represents the possible intruder who got the unauthorized access to the resource.
e. AttackPattern: Attack Patterns refers to the description of common methods that could be used by attackers and this could provide guidance on ways to mitigate their effect.
f. Exploit: This class characterizes description of an individual exploit.
g. Exploit Target: Exploit Targets are vulnerabilities in the systems that are targeted for exploitation.
h. Time Stamp: Time stamp when the event started and ended.

Intended Outputs

- Identification of cyber threats to specific railway assets (includes physical and cyber assets).
- Development of standard threat assessment processes / profiles for different classes of railway asset - output: library of threat assessment techniques appropriates for use with different railway asset profiles.
- Identification of best-practice responses to cyber threats in a range of candidate domains - output: a collection of best-practise case-studies of responses to identified cyber threats

B. Documentation of Cyber Security standards

Cyber Security standards need to be developed that define accessibility of rail assets to different rail stakeholder groups. This is tantamount to the creation of protected profiles that could be provided with privileged access to remotely monitor cyber assets. Protection Profiles could be defined in Common Criteria standard to characterize security and safety of elements/subsystem that compose a generic system framework. Resilience to cyber-attacks requires technical, procedural, and policy changes to the infrastructure, architecture, and enterprise operations. For any system, a threat analysis begins with the identification of the primary threats (any events that could directly cause loss); The unwanted trigging of a sensor is not a primary threat, however "Train delay due to some ones foul play with sensor" is a primary threat as it causes delays, financial loss, and damage to the reputation of the industry. According to Buldas a system is said to be "practically secure" against rational attacks if every primary threat is unlikely, i.e. non-profitable for attackers. The major elements of Cyber standards for rail assets have been identified and summarized in the table below. An existing effort to generate processes in this domain is underway at the Centre as part of the EPSRC-funded SCEPTICS project, [22]. The details of documentation have been omitted for simplicity.

TABLE II. KEY ELEMENTS FOR CYBER SECUIRTY

		Components of an Information System					
Security Goal		**Information**	**People**	**Processes**	**Hardware**	**Software**	**Networks**
Accountability	An ability of a system to hold users responsible for their actions (e.g. misuse of information)		X				
Auditability	Ability of a system to conduct persistent, non-by passable monitoring of all actions. performed by humans or machines within the system			X			
Authenticity/Trustworthiness	An ability of a system to verify identity and establish trust in a third party and in information it provides	X	X	X	X	X	X
Availability	A system should ensure that all system's components are available and operational when they are required by authorized users	X	X	X	X	X	X
Confidentiality	A system should ensure that only authorized users access information	X					
Integrity	A system should ensure completeness, accuracy, and absence of unauthorized modifications in all its	X	X	X	X	X	X
Non-repudiation	An ability of a system to prove (with legal validity) occurrence/non-occurrence of an event	X		X			
Privacy	A system should obey privacy legislation and it should enable individuals to control, where feasible, their personal information	X	X				

Cherdantseva [9] surveyed and prepared guidelines for security goals that need to be followed by various components of an information system. Table II and Table III represents security features and key entities around which protection profiles for railway applications needs to be developed [9]. Cyber security documentation is being created for different assets with a major emphasis on Point machines and Railway Track Signalling systems.

TABLE III. KEY ELEMENTS FOR CYBER STANDARD DOCUMENTATION

People	Areas such as Staff Competency and Contractor Competency
Product	Areas such as key Inspections and Maintenance Activities
Process	Areas such as Rail Defect Management, the TANC Process, the Fault Management
Asset Condition	Areas such as issues highlighted by the Asset Condition Report/Risk Register and emerging trends highlighted in the APRM/Performance reports

C. Cyber Ontology for Rail Assets

A three level rail asset ontology encompassing domain level, device level, and security level model has been proposed for this framework. Ontologies have been developed for various rail equipment's and corresponding data sets[13]. Sensor data, gathered via the IoT can be associated with asset instances in the triple store via in-memory database such as REDIS[17], buffering the high-throughput data and preventing excessive triggering of reasoning over the ontology instance. The idea here is to reuse the existing ontologies and make them scalable to incorporate a cyber ontology layer [10]. The details of same have been omitted in this research paper.

D. Improved FMEA (Failure Mode Effect Analysis)

Analysis of most common reasons for failure, as well as failure trends and correlations is done using FMEA techniques. It has been observed that FMEA and other related techniques do not include the check for deliberate failures [10]. Improved FMEA has been proposed for cyber assets through the inclusion of a failure mode type for "cyber failure" that captures the *concept* of a cyber threat. The security level ontology data could be used to measure the trust factor, potentially in conjunction with other existing models in this area. FMEA analysis is being done for European funded project PCIPP [11]. The idea is to improve FMEA for incorporating faults generated by cyber-attacks. The details of FMEA have been omitted in this paper and would be published soon.

III. CONCLUSION

In this research work a rail asset management framework has been proposed that emphasis protection profile generation for rail assets and showcases use of ontology to detect the tell-tale signs of cyber-attacks against industrial assets. Regarding future work we envisage the development of a standards-based, best practices database with implicit security knowledge in order to secure vulnerable Rail assets.

ACKNOWLEDGMENT

Work is being down under the University effort to develop Cyber Security Framework that could be showcased as university's ability to manage cyber security European Funded Projects.

REFERENCES

[1] C. Pu,"A world of opportunities: CPS, IOT, and beyond", In Proceedings of the 5th ACM international conference on Distributed event-based system, 2011, July, pp. 229-230.

[2] A. Cárdenas, S. Amin, S. Sastry, "Research Challenges for the Security of Control Systems", In HotSec, 2008, July.

[3] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry,"Challenges for securing cyber physical systems", In Workshop on future directions in cyber-physical systems security, 2009, July, p. 5.

[4] Combs, M. Marcia,"Impact of the Stuxnet Virus on Industrial Control Systems", XIII International Forummodern Information Society Formation Problems, Perspectives, Innovation Approaches,2011,5-10.

[5] US Rail Attack, http://www.nextgov.com/cybersecurity/2012/01/hackers-manipulated-railway-computers-tsa-memo-says/50498/

[6] A. Effendi, R. Davis,"ICS and IT: Managing Cyber Security Across the Enterprise", In SPE Middle East Intelligent Oil and Gas Conference and Exhibition. Society of Petroleum Engineers,2015

[7] Lee, Robert M., Michael J. Assante, and Tim Conway. "German Steel Mill Cyber Attack." Industrial Control Systems 30 (2014).

[8] Network Rail. "Cyber Security Strategy September 2013".2013. https://www.networkrail.co.uk/WorkArea/DownloadAsset.aspx?id=30064788605

[9] Y. Cherdantseva, J. Hilton,"A reference model of information assurance & security", In Availability, reliability and security (ares), 2013 eighth international conference on, pp. 546-555. IEEE, 2013.

[10] R. Lewis, F. Fuchs, M. Pirker, C. Roberts, G. Langer,"Using ontology to integrate railway condition monitoring data", In Railway Condition Monitoring, 2006. The Institution of Engineering and Technology International Conference on (pp. 149-155). IET.

[11] S. Kohli , J.M. Easton,"PCIPP: An Approach for Predictive Maintenance of Railway Assets", International Conference on Railway Engineering 2016 (ICRE), *In press*

[12] NIST,http://www.nist.gov/cyberframework/

[13] Tutcher, J., 2014, October. Ontology-driven data integration for railway asset monitoring applications. In Big Data (Big Data), 2014 IEEE International Conference on (pp. 85-95). IEEE.

[14] M. C. Morris, J. M. Easton, C. Roberts,"Ontology in the Rail Domain", 7th International Joint Conference on Knowledge Discovery, Knowledge Engineering, and Knowledge Management,2015

[15] A. Buldas, P. Laud, J. Priisalu, M. Saarepera, J. Willemson," Rational choice of security measures via multi-parameter attack Trees",In Critical Information Infrastructures Security,2006, pp. 235-248, Springer Berlin Heidelberg

[16] R. Bloomfield, I. Gashi,R. Stroud,"How secure is ERTMS?", In Computer Safety, Reliability, and security , 2008, pp. 247-258, Springer Berlin Heidelberg.

[17] REDIS,https://redislabs.com/

[18] M. Abrams, J. Weiss,"Malicious control system cyber- security attack case study–Maroochy Water Services", Australia. McLean, VA: The MITRE Corporation,2008.

[19] A. Cardenas, A. Saurabh, S. Sastry, "Secure control: Towards survivable cyber-physical systems.", In The 28th International Conference on Distributed Computing Systems Workshops, pp. 495-500. IEEE, 2008.

[20] L. Obrst,P. Chase, R. Markeloff," Developing an Ontology of the Cyber Security Domain", In STIDS, 2012, October,pp. 49-56.

[21] S. Caltagirone, A. Pendergast, C. Betz,"The diamond model of intrusion analysis",Center for cyber intelligence analysis and threat research hanover md, 2013.

[22] R. Evans, J. Easton, and C. Roberts, "SCEPTICS: A Systematic Evaluation Process for Threats to Industrial Control Systems", in Press, World Congress on Railway Research, 29th May - 2nd June 2016, Milan, Italy.