Proceedings of the Sixth International Conference on
Railway Technology: Research, Development and Maintenance
Edited by: J. Pombo
Civil-Comp Conferences, Volume 7, Paper 23.4
Civil-Comp Press, Edinburgh, United Kingdom, 2024
ISSN: 2753-3239, doi: 10.4203/ccc.7.23.4

CyRail: Enhancing Cybersecurity in Railway Operational Technology Through an Innovative Software Assistant

R. Bolton[1], D. Basher[1], S. Parkinson[2] and H. Parkinson[1]

[1] **Digital Transit Limited, Digital Transit Limited Lancaster, UK**
[2] **Institute of Railway Research, School of Computing and Engineering, University of Huddersfield, UK**

Abstract

The cybersecurity of operational technology continues to be a dominant challenge. New threats are evolving and there is a widespread skill shortage. This continues to put railway technology at significant risk. In response, the CyRail project is an innovative venture aimed at advancing cybersecurity in railway operational technology by overcoming skill shortages through the use of artificial intelligence. The project aims to create intelligent software that is tailored to the unique cybersecurity needs of the railway sector. This includes providing assistive technology capable of understanding and implementing cybersecurity standards by leveraging advanced natural language processing, particularly large language models.

The CyRail methodology involves the application of existing cybersecurity frameworks and standards with the specific demands of railway operational technology, facilitated by a user-friendly interface and expert guidance provided by large language models. This approach has shown significant potential to improve the ease of navigating complex cybersecurity regulations and enhance threat detection and mitigation capabilities. The implications of CyRail for railway operational technology cyberse-

curity are profound. It represents a shift toward more accessible, proactive, and integrated cybersecurity management within the railway industry. This product could set a new standard in how cybersecurity is managed, promoting a safer and more secure future for railway operations.

Keywords: cyber-security, operational technology, generative artificial intelligence, large language model, cyber-security management system, guideline compliance, retrieval augmented generation.

1 Introduction

The railway sector is increasingly embracing digitalisation, integrating advanced technologies such as the Internet of Things (IoT), automation systems and digital communication networks into its operations. This shift to digital technology has demonstrated improvements in operational efficiency, safety, and passenger experience. However, it also introduces a new array of cybersecurity challenges, particularly in Operational Technology (OT) systems that are crucial to the safe and reliable functioning of railway infrastructure [1]. OT systems in railways, including signal systems, train control, and track monitoring technologies, are different from traditional IT systems in their functionality and security requirements. Not only are these systems operating in safety-critical systems, they are often a blend of older, legacy technologies and modern digital solutions, making them vulnerable to well-documented and easily exploited cybersecurity threats. The integration of these systems with technologies enabled by the Internet has exposed them to risks previously not encountered in the sector. As railway systems are highly connected, many of the threats facing railway systems involve network weaknesses [2].

Control systems that are not secure against cyber-attacks are vulnerable and cannot be considered safe. In other words, “If it is not secure, then it is unlikely to be safe” [3]. The relationship between cybersecurity and functional safety is outlined in Figure 1.

Rail is similar to other industries in terms of safety regulation; however, it is unique in terms of cybersecurity, as it consists of extensive business premises that are widely accessible to the public with infrastructure that can span entire countries or continents [4, 5]. ITCS (Information Technology CyberSecurity) has been managed in rail OT with the adoption of the ISO27000 [6] suite of standards, and in this way, railway business systems are not too dissimilar to other industries. However, the Operational Technology Cyber Security (OTCS) rail systems are lagging behind other industries such as aviation [7] and could be vulnerable to attack. Figure 2 shows the delimitation between OTCS and ITCS as described in TS50701 [8].

To help understand why cyber security in rail systems has not progressed as much as in other industries, it is important to consider the complex threat landscape that exists in the railways. The railway has a substantial amount of technology that is specific to the rail domain. These systems can have operating lifetimes of 30 or more years [7].

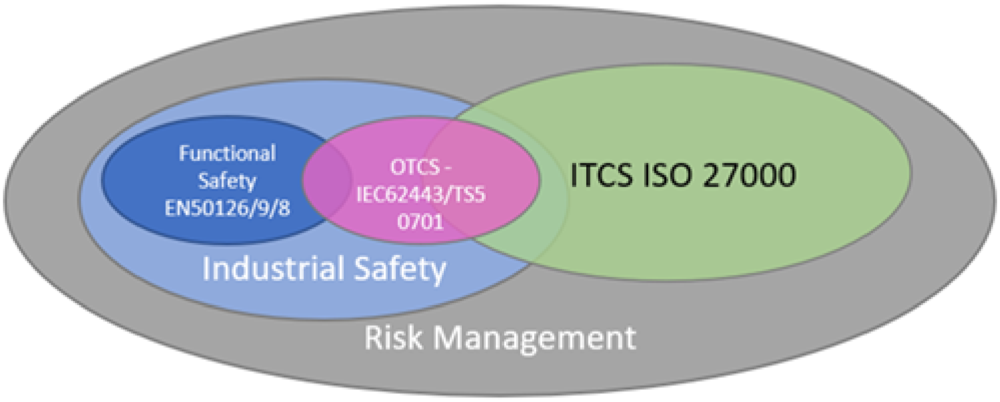

Figure 1: A diagram outlining the relationship between cybersecurity and safety.

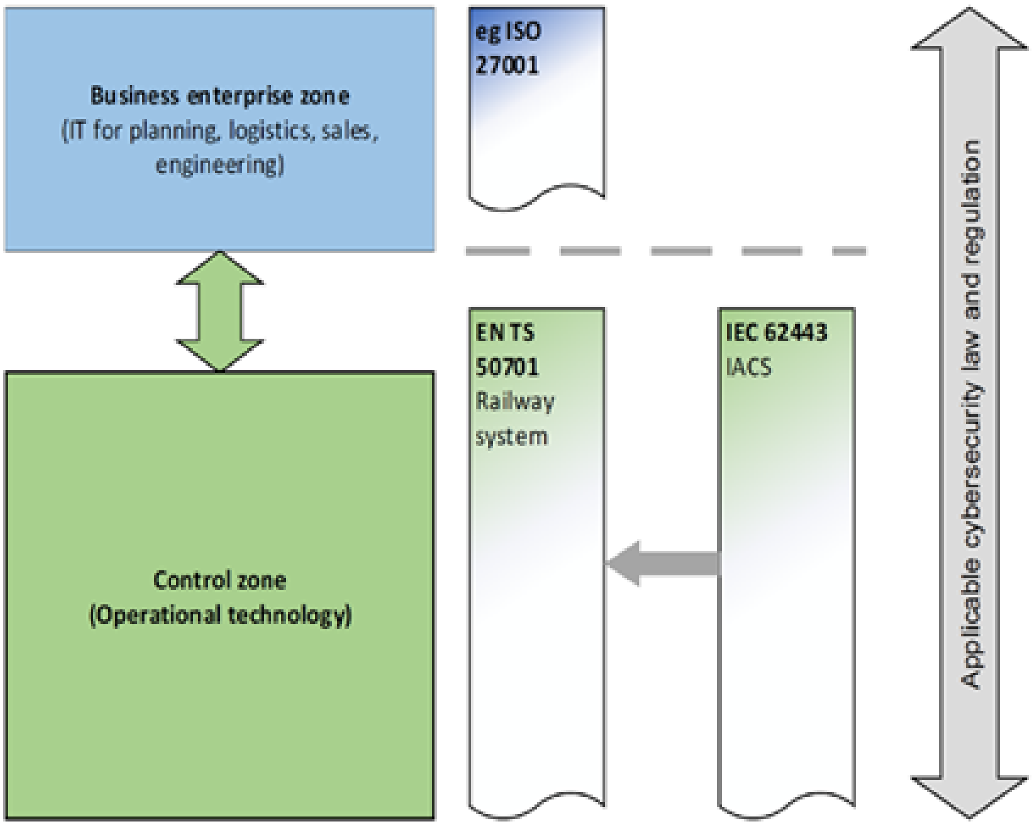

Figure 2: A diagram showing the OTCS (green) and ITCS (blue) relationship according to TS50701 [8]

Furthermore, as the digitalisation of the railway continues, the threat surface will only continue to grow. This digitalization occurs through the implementation of new technologies, many of which are commercial off-the-shelf (COTS) and bring with them an increased chance of exposure to a cyber attack [9]. Due to the long lifetime of rail systems, most existing systems are legacy systems that were not designed with a modern understanding of cybersecurity in mind [10]. This complexity can be navigated by following standards and industry research. In this context, CyRail emerges as a pioneering initiative. CyRail provides a specialised software assistant to enhance cybersecurity in railway OT by leveraging advanced natural language processing and Large Language Models (LLMs).

LLMs have already been used to automatically detect malicious phishing emails [11], highlighting a successful use case in cybersecurity. This demonstrates their analytical capability, and we propose that LLMs can be used as a tool to simplify and make sense of cybersecurity guidelines for the average nontechnical user. Furthermore, we can use LLMs to analyse the compliance of the CyberSecurity Management System (CSMS) documentation with these guidelines. These two components of our system can boost cybersecurity where it is desperately needed, in the rail sector.

CyRail is designed to navigate complex cybersecurity challenges specific to the railway industry. By providing targeted guidance and tools for cybersecurity management, CyRail seeks to bridge the gap between the traditional robustness of rail systems and the demands of modern cybersecurity, ensuring a secure transition into the digital era of rail transport. This paper lays the foundations for CyRail, explaining and motivating its development. First, the differences between OT and IT are discussed in a cybersecurity context, which is necessary to provide a background on the challenges being addressed in the CyRail project.

2 Differences Between OT and IT in Cybersecurity

Operational Technology (OT) and Information Technology (IT) in railways serve different functions and face different cybersecurity challenges. IT systems focus on data confidentiality and integrity, while OT prioritises the physical operation of railway systems, focussing on safety and availability. The inherent differences in design and purpose between these two technologies require unique approaches to cybersecurity. Traditional IT security technologies are not often designed taking into account the cybersecurity requirements of OT [12].

2.1 Cybersecurity Challenges in Railway Systems

Railway systems are increasingly integrating digital technologies with existing OT infrastructure, leading to new cybersecurity vulnerabilities. The blend of legacy and modern railway systems creates a complex security landscape, where traditional IT security solutions are often insufficient. This integration poses significant challenges, making railway OT systems more susceptible to cyberattacks that can disrupt operations and compromise safety. Furthermore, legacy technology and disparate devices result in a series of complex cybersecurity requirements [7].

The most famous OT attack was Stuxnet, a highly sophisticated and malicious computer worm first discovered in 2010. It is notable for being one of the first known worms developed to target industrial control systems (ICS) and operational technology (OT) rather than just traditional computers or networks. Its discovery marked a significant moment in the history of cybersecurity and cyber warfare due to its complexity and the specific nature of its target [13]. In terms of cybersecurity attacks, the following list provides three typical known and significant attacks:

- San Francisco Municipal Transportation Agency (SFMTA) Ransomware Attack (2016): The SFMTA was hit by a ransomware attack that encrypted important databases. While it did not affect actual train services, it caused significant operational problems, including the disabling of ticket machines across the network.
- Deutsche Bahn WannaCry Ransomware Attack (2017): The German railway company Deutsche Bahn was one of the many victims of the global WannaCry ransomware attack. This attack caused the disruption of digital display panels at train stations and other minor operational inconveniences.
- Swedish Transport Administration Cyberattack (2017): In Sweden, a cyber attack targeted the Transportation Administration, affecting railway communications and leading to delays and cancelations of train services.

These incidents highlight the growing need for robust cybersecurity measures in rail systems to protect against operational disruptions and potential safety hazards.

3 The use of Large Language Models in CyRail

The integration of Large Language Models (LLM) in CyRail is a novel strategy aimed at strengthening cybersecurity in railway operating technology (OT). These models adeptly parse and interpret vast amounts of cybersecurity documentation, extracting key insights and actionable guidelines tailored to the unique needs of railway OT systems. This approach considerably simplifies the understanding and application of complex security protocols, making them more accessible to various users in the railway industry.

The utilisation of LLMs in CyRail has distinct advantages. Firstly, their ability to quickly process and understand large data sets enables a comprehensive analysis of cybersecurity documents, standards, and protocols. This rapid processing facilitates quicker decision-making and implementation of necessary security measures, crucial in the dynamic field of railway OT. Furthermore, LLMs in CyRail can identify subtle patterns and correlations in data that human analysts might overlook, thus enhancing the depth and quality of cybersecurity analysis. However, the deployment of LLMs in

CyRail is not without its challenges and limitations. One notable concern is the potential for conflicting information in different, perhaps older cybersecurity regulations, which could skew results and recommendations.

A review has been conducted to assess the work that is being done using LLMs to facilitate engineering decision-making and compliance evaluation.

3.1 LLMs Within Engineering For Decision-making

Artificial intelligence (AI) within the engineering sector is already being used to make informed decisions in control systems. A study addresses the integration of AI in various aspects of control systems to improve operational performance and improve the decision-making process [14]. This demonstrates the potential of using a range of AI systems for informed decision-making within the engineering sector. LLMs are already being used to make informed decisions, for example, a study uses a model titled Language MPC to make autonomous driving decisions [15]. This work demonstrates how LLMs have human-like reasoning capabilities that can effectively provide decision-making in real-time while driving. They demonstrate how LLMs can revolutionise autonomous driving technology.

3.2 Existing LLMs For Guideline Compliance and Advice

One of the main objectives of CyRail is to help ensure compliance with rail cybersecurity standards. Although there are currently no examples of LLM compliance evaluation in the rail sector, the automotive industry has undertaken this type of compliance. An example is the design compliance assessment in automotive control software [16], which details the use of a neural language model, trained in source code, to perform compliance evaluation. A second example, in the medical field, involves an investigation of how compliance can be assessed against reporting guidelines in clinical trials [17]. The findings showed that AI-LLM demonstrated an acceptable classification accuracy performance to assess guideline compliance. Interestingly, this article used prompt engineering to complete its task; the given example was as follows: "You are a health researcher reviewing a scientific article for a peer-reviewed sports medicine journal. You will be supplied with the text of the article and a question (delimited by XML tags). Use the text of the article to answer the question. You must answer the question in steps. Delimit each step. Step 1: Summarise the information in the text relevant to the question. Step 2: Answer the question 'YES' or 'NO'. Following this framework, we can see how the prompts can be designed to tailor our LLM's purpose of maturity scoring and guidance. Another interesting attribute of this paper is the method of data extraction; they split up their case study articles into sections and for each section applied a (text, question) pair to match the reporting guidelines with a labelled YES or NO depending on the compliance. This is a technique called fine-tuning; CyRail uses a similar technique for the evaluation of standards compliance.

3.3 The Integration of Large Language Models in Cyrail

Security copilots with retrieval-augmented generation (RAG) enable organisations to take advantage of existing knowledge bases and extend the capabilities of human analysts, making them more efficient and effective. By 2025 it is estimated that two-thirds of businesses will leverage a combination of generative AI and RAG to power domain-specific self-service knowledge discovery, to improve decision efficacy [18]. Using RAG and other techniques, such as fine-tuning and prompt engineering, we can define our LLM training pipeline. This gives us confidence that our LLM will have a high confidence level for expert knowledge queries and analysis once these techniques are developed.

In summary, LLMs are a transformative tool in CyRail and can be used as a powerful expert knowledge system for queries and compliance analysis. Ongoing efforts to refine these models and tailor them to the specific needs of the railway industry are crucial to maximising their effectiveness and reliability in improving OT cybersecurity.

4 CyRail Overview

The CyRail project is an initiative designed to improve cybersecurity in railway OT. It aims to bridge the gap between traditional cybersecurity approaches and the specific needs of railway OT systems. CyRail is envisioned as a tool that uses advanced natural language processing, particularly LLM, to provide guidance and support in navigating the complex landscape of cybersecurity regulations and practices in the railway sector.

4.1 Aims and Objectives

The primary objective of CyRail is to improve the cybersecurity posture of railway OT systems. This is to be achieved through several key aims and objectives:

- **Enhanced Understanding of Cybersecurity Practices:** By simplifying complex standards and regulations, CyRail aims to make cybersecurity more accessible to railway professionals, regardless of their technical background.
- **Threat Risk Management and Mitigation:** The project seeks to equip railway operators with the tools necessary to identify potential cyber threats and take pre-emptive actions to mitigate them.
- **Detailed Analysis of Existing Cybersecurity Documentation:** Using a standard taxonomy, CyRail aims to evaluate existing CSMS and suggest the necessary improvements to rail professionals.
- **Document Builder:** If an organisation does not have a CSMS, there should be a process to create the relevant documentation easily.

	Cybersecurity related	Software related	Systems related	Safety related	Organisation related
Corporate	ISO 27001	ISO/IEC 12207 (software development)	ISO/IEC 15288 (system engineering)		ISO 9001 (quality management)
	NIST Cybersecurity Framework	ISO/IEC 15288 (system engineering)	ISO 55000 (asset management)		ISO 21827 (security CMM)
Operational	IEC 62443 series (OT cyber processes)	IEC 61508 (functional safety sw)	ISO 19439 (systems modelling)	IEC 61508 (functional safety sw)	
	NIST SP800-82 (OT cyber processes)				
Rail specific	TS 50701 (rail cyber processes)	EN 50128 (rail software engineering)		EN 50126 (rail RAMS)	
		EN 50155 (rail software testing)		EN 50129 (rail safety file)	

Table 1: CyRail related guidelines taxonomy

- **Integration with Existing Guidelines and Standards:** CyRail is engineered to be in alignment with prominent cybersecurity best practices, such as the NIST Cybersecurity Framework [19], ISO 27001 IT Cybersecurity standard, [3], and sector-specific standards such as the IEC 62443 series [20]. This alignment ensures that CyRail's guidance and risk assessment methodologies are grounded in globally recognised best practices. The considerations for additional guidelines can be seen in Table 1.

4.2 Architecture

The CyRail system architecture (illustrated in Figure 3) is designed around our core aims and objectives, addressing the specific cybersecurity needs of the railway OT

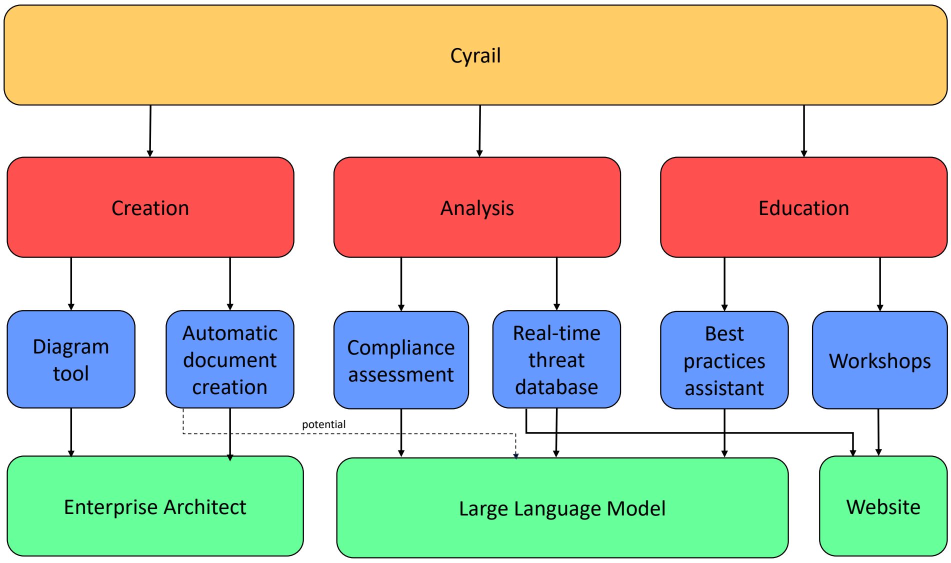

Figure 3: A diagram showing the components of the project and the relationship between them.

systems. The core framework involves:

- **A best practices assistant** to ingest and overview complex cyber security guidelines for non technical users. Using a RAG based approach we can quickly analyze complex standards and make requirements easy to understand.
- **A compliance assessment tool** to assess the maturity of user documentation based on these guidelines. Using a similar methodology to the best practices assistant this tool additionally makes use of a PDF ingestor and RAG to provide an analysis of a cybersecurity documentation.
- **Real-time threat database** to actively monitor emerging threats on the website and as an input to the compliance assessment.
- **A creation tool** to accelerate cybersecurity diagram and documentation creation. Interfacing with Enterprise Architect, we completely model OT cybersecurity guidelines using a custom modeling language. This helps users rapidly build relevant CSMS documentation.
- **Workshops and resources** to educate businesses in the rail industry so that OT cybersecurity is taken more seriously in the industry, demonstrated on our website.

4.3 Development overview

CyRail has followed a methodical approach to its development that involves several key phases.

- **Research and Analysis:** The initial phase involves a comprehensive investigation of existing cybersecurity frameworks and the specific challenges faced by railway OT systems. This includes analysing past cyberattacks in the railway sector to identify common vulnerabilities and threats.

- **Development of the best practices assistant:** This involves using RAG, prompt engineering and fine tuning to understand and interpret various cybersecurity best practices.

- **Development of the maturity assessment tool:** This involves building upon the framework of the best practices assistant to include document ingestion and compliance-related interpretation of documentation.

- **Development of the creation tool:** Another avenue that the product addresses is the creation of cybersecurity documents. Interfacing with Enterprise Architect, CyRail will completely automate the creation of required documentation related to the CSMS.

- **User Interface Design:** A significant focus is placed on designing an intuitive user interface that allows easy navigation and interaction with system components, making cybersecurity assessment and compliance accessible to all users.

- **Integration of system components:** Each of the different components and systems interacts with each other. All components are integrated into the web server and are properly formatted in the UI to ensure usability.

- **Testing and Iteration:** CyRail has undergone rigorous testing, including beta testing with real-world users, to refine its functionality and ensure its effectiveness in different operational environments.

- **Deployment and Feedback Integration:** Finally, the system is installed for use in the railway sector, with continuous feedback mechanisms in place to allow ongoing improvements and updates in response to evolving cybersecurity threats and user needs.

CyRail's architecture is designed to ensure that it not only addresses the current cybersecurity challenges in the railway sector, but is also adaptable and effective in the face of an evolving landscape of cyber threats. This comprehensive system, with its focus on user accessibility, positions CyRail as a leading solution to enhance the cybersecurity resilience of railway OT systems.

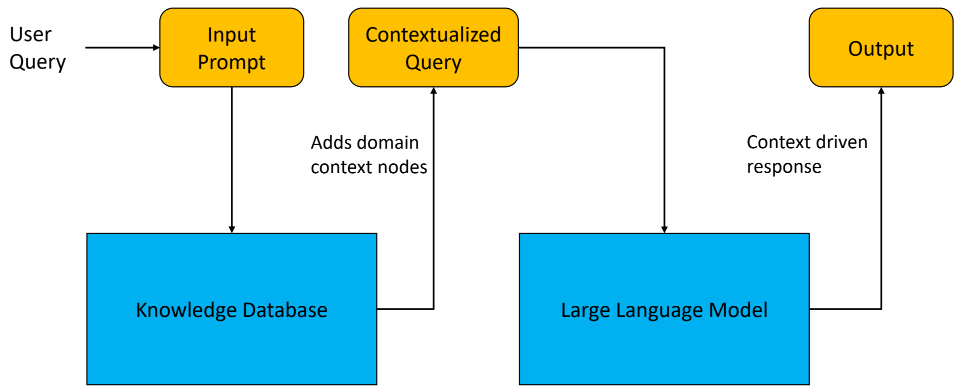

Figure 4: A diagram showing the process of RAG in our best practices assistant.

5 Methodology and Results

In this section we describe the methodology and current developmental work completed for the project.

5.1 Best practices assistant

The Best Practices Assistant leverages a comprehensive database of guidelines and standards, organized into discrete nodes of information. This knowledge database forms the backbone of our retrieval engine, which can discern and retrieve the best practices in response to user queries. For instance, if I were to query the assistant related to how to partition my system under consideration, the engine would efficiently identify and retrieve the relevant nodes in relation to this topic.

Upon gathering the necessary information from the knowledge database and receiving a user query, this data is processed through an LLM. Using the query and context an LLM can easily interpret the standards and provide a range of useful responses. This functionality remains robust even in the face of complex user queries. The approach and its underlying methodology are further illustrated in Figure 4, where we deconstruct our Retrieval-Augmented Generation (RAG) process.

For our system we used the model LLama2-7b-chat [21], this is an open source model created by Meta which is trained on over 2 trillion tokens, meaning that it has a very good existing understanding of language. Currently, we have created a prototype assistant and have been evaluating its performance by asking complex questions

Query	Response
What is the relationship between the cybersecurity case and the cybersecurity requirements specification in railway cybersecurity management system?	The cybersecurity case and the cybersecurity requirements specification are closely related in railway cybersecurity management system. The cybersecurity case provides the evidence and argumentation that the system as designed and developed can be operated to the expected security confidence level, while the cybersecurity requirements specification defines the security objectives and requirements for the system. The cybersecurity case is built upon the results of the threat risk assessment and the cybersecurity requirements specification, and it provides the assurance evidence of the system's compliance with the security requirements. In other words, the cybersecurity case is the tangible output of the cybersecurity requirements specification, and it serves as the basis for the system's operation and maintenance.
What is the role of the system integrator in a railway cybersecurity management system?	The system integrator plays a crucial role in railway cybersecurity management system by providing a comprehensive approach to cybersecurity that includes risk assessment, security design, implementation, testing, and integration of security solutions with existing systems. They help to identify potential vulnerabilities and threats to the railway system and develop strategies to mitigate them. They also work closely with the railway operators to ensure that the security solutions are integrated into the existing systems and are functioning effectively. Additionally, they provide ongoing monitoring and maintenance of the security solutions to ensure that they are up-to-date and functioning optimally.
How can i prevent unauthorised access to my Secure Train Integrity Monitoring Systems	1. Implement secure boot mechanisms to ensure only authorized software is permitted and executed. 2. Limit USB ports usage and employ USB controller and OS driver hardening to prevent execution of code from USB devices. 3. Use a white list application management at operating system/firmware and application layers to prevent execution of unauthorized software. 4. Implement invalidation of session IDs after session termination to prevent unauthorized access. 5. Generate unique session IDs and ensure their randomness to prevent unauthorized access. 6. Protect audit information and ensure its confidentiality, integrity, and availability. 7. Implement secure defaults and secure metadata management to prevent unauthorized access. 8. Control access to sensitive information and assume secrets are not safe. 9. Promote privacy and implement security measures to protect sensitive information.

Table 2: CyRail best practices assistant example query answers

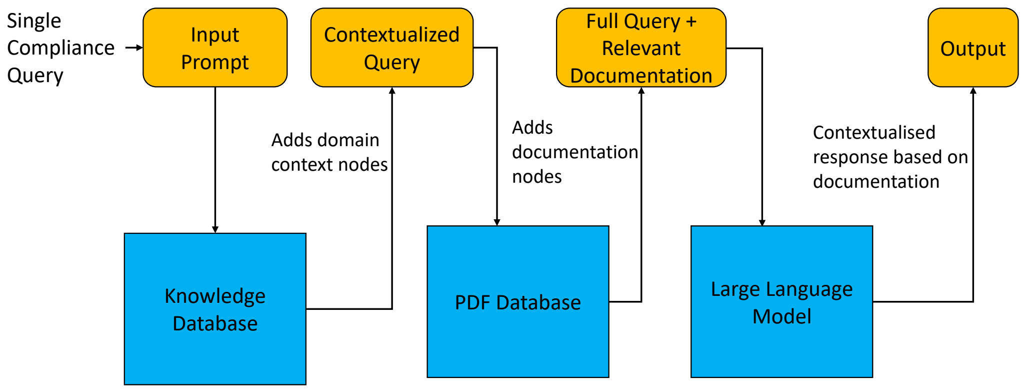

Figure 5: A diagram showing the process of our compliance assessment

regarding IEC 62443 and TS50701 standards.The preliminary results, as documented in Table 2, demonstrate the assistant's proficiency in understanding complex questions and providing relevant responses, even without the application of additional optimization strategies such as fine-tuning and prompt engineering. These outcomes are promising, and as we advance in refining the Best Practices Assistant, we anticipate a continued enhancement in the response quality.

5.2 Compliance assessment tool

The development of the Compliance Assessment Tool is currently underway, and while a working prototype is not yet available, it expands upon our existing Best Practices Assistant by incorporating a new PDF Ingestor component. This addition is crucial given the nature of CSMS documentation, which often spans multiple extensive documents. To address the limitations posed by large volumes of text, such as the tendency of Large Language Models (LLMs) to overlook details in longer inputs, we employ another RAG based methodology. This strategy is designed to minimize token consumption and enhance the specificity of queries.

Building on the principles established by the Best Practices Assistant, we query the system several times with targeted, compliance-related questions. An example of such a query could be, ”Are there any policies and procedures in place for screening personnel in security-sensitive roles?” In response, the system initially extracts domain-specific data from the knowledge database. Subsequently, a secondary RAG retrieval engine sources the documentation from the PDF database, collecting the targeted cybersecurity personnel documentation.A detailed system overview can be seen

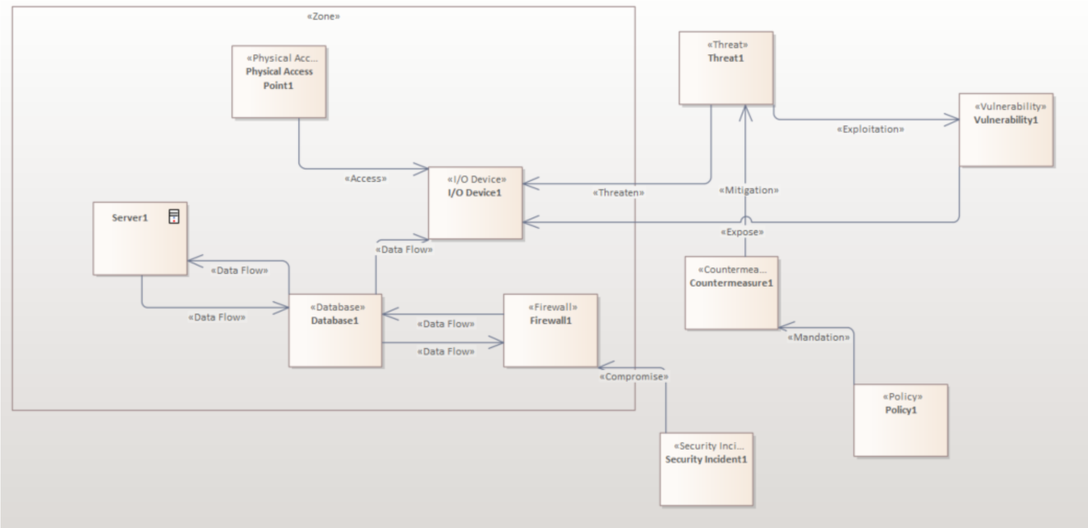

Figure 6: A prototype of the modelling language used in the creation tool

in Figure 5.

One of the key advantages of this method is its inherent scalability, allowing for simultaneous processing of multiple queries. This capability significantly enhances the efficiency of generating a comprehensive compliance document from the outputs of these compliance-related queries. In future work, we intend to integrate real-time threat intelligence into our domain knowledge base, refining the tool's effectiveness in navigating the ever-changing threat landscape.

5.3 Creation tool

The development of our Creation Tool represents a significant advancement in the domain of OT cybersecurity by introducing a bespoke modeling language. This language is underpinned by the IEC 62443 standards, encompassing a variety of modifiable elements such as assets, zones, conduits, threats, countermeasures, policies, and security incidents, along with their intended relationships.

Creating an extensive modelling language allows us to do many things, mainly describing the relationships between each of the components within the CSMS. An extensive example of all component relationships can be seen in Figure 6. By leveraging these relationships, we are able to transform visual data into meaningful textual descriptions.

These textual representations offer numerous benefits. Among these is the capability for such representations to be analysed by our compliance assessment tool. Moreover, the integration with Enterprise Architect's custom documentation feature facilitates the generation of templated documentation based on system diagrams. This is extremely useful in producing essential documentation for a compliant CSMS.

Future work may include the complete automation of CSMS documentation. This would involve leveraging LLM techniques automate the documentation creation process, signifying a leap towards more autonomous and streamlined compliance management within cybersecurity frameworks.

6 Conclusions & Contributions

Initially we examined the current landscape of OT cybersecurity within the rail industry, supplemented by a comprehensive literature review on the application of LLMs in cybersecurity and general LLM compliance in other neighbouring sectors. Following this foundational analysis, we delved into a detailed description of our system architecture, focusing on its principal components.

Our work includes innovative methodologies for the management of cybersecurity documentation, employing LLMs to not only interpret to but also adhere to the overarching guidelines for OT cybersecurity. Once developed, we expect that our findings can be applied to many different cybersecurity sectors and even in other domains for different compliance-related documentation.

CyRail marks a significant advancement in addressing the cybersecurity needs of railway Operational Technology. We aim to completely automate the cybersecurity management process to alleviate the burden of regular cybersecurity management and set a new standard of documentation. As CyRail evolves, it will continue to play a vital role in the proactive management of cybersecurity risks in the railway industry, [1, 8] contributing to safer and more secure transportation networks.

References

[1] R. Kour, A. Patwardhan, A. Thaduri, and R. Karim, "A review on cybersecurity in railways," *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, vol. 237, no. 1, pp. 3–20, 2023.

[2] D. Unwin and L. Sanzogni, "Railway cyber safety: An intelligent threat perspective," *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, vol. 236, no. 1, pp. 26–34, 2022.

[3] "Information security management iso/iec 27000," 2018.

[4] S. G. PREDESCU, S. Daniel, and V. E. BADEA, "Cybersecurity in the railway sector."

[5] S. Unger, M. Heinrich, D. Scheuermann, S. Katzenbeisser, M. Schubert, L. Hagemann, and L. Iffländer, "Securing the future railway system: Technology forecast, security measures, and research demands," *Vehicles*, vol. 5, no. 4, pp. 1254–1274, 2023.

[6] "Enr135 – v1 - taking cybersecurity challenges into account in railway safety," 2021.

[7] R. Kour, M. Aljumaili, R. Karim, and P. Tretten, "emaintenance in railways: Issues and challenges in cybersecurity," *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, vol. 233, no. 10, pp. 1012–1022, 2019.

[8] "Rail cyber security guidance to industry," 2016.

[9] "Clc/ts 50701 railway applications - cybersecurity," 2023.

[10] R. Bloomfield, M. Bendele, P. Bishop, R. Stroud, and S. Tonks, "The risk assessment of ertms-based railway systems from a cyber security perspective: Methodology and lessons learned," in *Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification: First International Conference, RSSRail 2016, Paris, France, June 28-30, 2016, Proceedings 1*. Springer, 2016, pp. 3–19.

[11] N. Sessions, "Bolstering cybersecurity: How large language models and generative ai are transforming digital security," Dec 2023.

[12] D. Parsons, "The state of ics/ot cybersecurity in 2022 and beyond," *Survey Report*, 2022.

[13] L. J. Trautman and P. C. Ormerod, "Industrial cyber vulnerabilities: Lessons from stuxnet and the internet of things," *U. Miami L. Rev.*, vol. 72, p. 761, 2017.

[14] D. A. Linkens, "Ai in control systems engineering," *The Knowledge Engineering Review*, vol. 5, no. 3, pp. 181–214, 1990.

[15] H. Sha, Y. Mu, Y. Jiang, L. Chen, C. Xu, P. Luo, S. E. Li, M. Tomizuka, W. Zhan, and M. Ding, "Languagempc: Large language models as decision makers for autonomous driving," *arXiv preprint arXiv:2310.03026*, 2023.

[16] D. Parthasarathy, C. Ekelin, A. Karri, J. Sun, and P. Moraitis, "Measuring design compliance using neural language models: an automotive case study," in *Proceedings of the 18th International Conference on Predictive Models and Data Analytics in Software Engineering*, 2022, pp. 12–21.

[17] J. G. Wrightson, P. Blazey, K. M. Khan, and C. L. Ardern, "Gpt for rcts?: Using ai to measure adherence to reporting guidelines," *medRxiv*, pp. 2023–12, 2023.

[18] H. S. Ritu Jyoti, David Schubmehl, "Idc futurescape: Worldwide artificial intelligence and automation 2024 predictions," 2023. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=AP50341323

[19] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule, and M. Thompson, "Nist sp800-82 csrc guide to operational technology (ot) security," Sep 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/82/r3/final

[20] "Iec62443 suite of standards," 2024. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[21] H. Touvron, L. Martin, K. Stone, P. Albert, A. Almahairi, Y. Babaei, N. Bashlykov, S. Batra, P. Bhargava, S. Bhosale, D. Bikel, L. Blecher, C. C. Ferrer, M. Chen, G. Cucurull, D. Esiobu, J. Fernandes, J. Fu, W. Fu, B. Fuller, C. Gao, V. Goswami, N. Goyal, A. Hartshorn, S. Hosseini, R. Hou, H. Inan, M. Kardas, V. Kerkez, M. Khabsa, I. Kloumann, A. Korenev, P. S. Koura, M.-A. Lachaux, T. Lavril, J. Lee, D. Liskovich, Y. Lu, Y. Mao, X. Martinet, T. Mihaylov, P. Mishra, I. Molybog, Y. Nie, A. Poulton, J. Reizenstein, R. Rungta, K. Saladi, A. Schelten, R. Silva, E. M. Smith, R. Subramanian, X. E. Tan, B. Tang, R. Taylor, A. Williams, J. X. Kuan, P. Xu, Z. Yan, I. Zarov, Y. Zhang, A. Fan, M. Kambadur, S. Narang, A. Rodriguez, R. Stojnic, S. Edunov, and T. Scialom, "Llama 2: Open foundation and fine-tuned chat models," 2023.