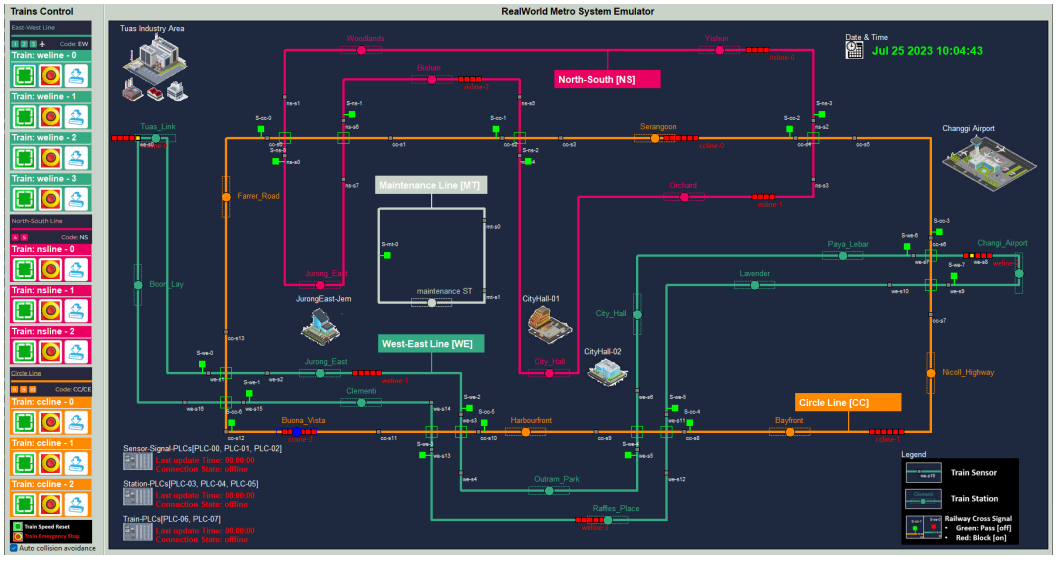
Introduction

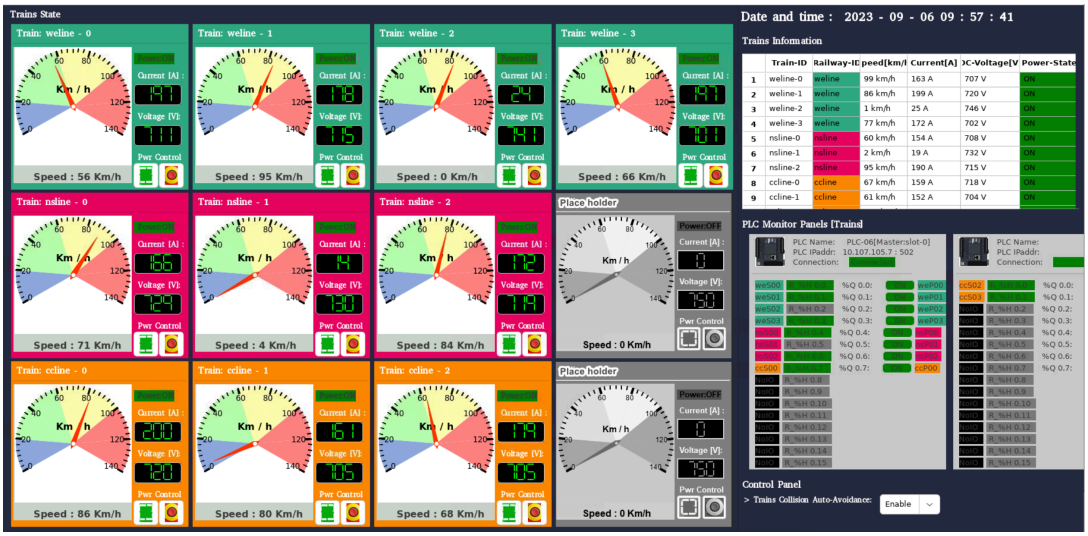
Railway [Metro] System was built in 2023 by NCL development team, for research in cyber security. Its purpose is to help ICS researchers and instructors test IT/OT attack and defense solutions and provide a platform for ICS security training and education.

Our idea on creating a digital version of the railway system emulation platform, designed to replicate the operation of multiple trains traversing distinct tracks, each equipped with unique sensor-signal controls. This platform is intended to serve as a valuable resource for cybersecurity researchers, enabling them to demonstrate and assess the impact of various types of IT attacks on operational technology (OT) systems. The platform comprises six primary components (programs):

- Railway [Metro] System
- Railway System SCADA HMI
- Railway System Train Controller HMI
- Railway Junctions Sensor – Signal System Control PLC Simulator
- Railway Stations Sensor – Signal System Control PLC Simulator
- Railway Trains Sensor – Power System Control PLC Simulator



Real-world Metro System Emulator



Railway System Train Controller HMI

Railway System SCADA HMI

What might this system be useful for:

- **Training and Education:** This system serves as an invaluable tool for educating students about Railway Systems, their components, and operational processes.
- **Testing and Validation:** The system can be employed to rigorously test and validate the effectiveness of products or assess the credibility of logical processes.
- **Security Testing:** For those interested in testing their skills at identifying vulnerabilities in railway systems, we offer a secure environment where you can engage in ethical hacking exercises.
- **Research and Development:** NCL also provides a diverse range of GPUs available for rent, enhancing the quality of your research and development efforts in the field of Railway Systems.

Collaboration

NCL is engaged in an international cybersecurity exercise, presenting our Railway System. Our railway infrastructure will serve as a live operational technology (OT) target for red team to exploit.

We have meticulously prepared a set of compelling attack scenarios, primed for demonstration. If you are intrigued and eager to learn more information, please feel free to reach out to us at:

Email:	support@ncl.sg
Address:	National Cybersecurity R&D Lab (NCL), School of Computing National University of Singapore COM3-B1-09, 11 Research Link, Singapore 119391