Group ID: 10-25

Future Trends Report
Based on Analysis of the Team's Chosen Community / Organisation in Mid-Term and Final Evaluation

Community / Organisation Studied: SMRT Trains Limited

STEP 1. Identify Challenges

Read the Future Scene carefully and generate ideas for challenges, concerns, and possible related problems. Choose the 5 most important challenges and write them in the space provided. Include applicable research with appropriate in-text citations.

Challenge #1:
Observation: Based on our interview with Prof. See, it is predicted and widely accepted that rail technology (trains, signalling systems etc) will become increasingly interconnected with the wider Internet, in the style of IoT (Internet of Things → 4th IR).

Why this observation could pose a problem: This will be a problem as it will make rail technology more vulnerable to external hackers, which give malicious hackers the chance to cause more damage to our transportation network, which could bring our country to a standstill instantly.

Research: According to an article by **CNBC [1]**, such attacks are not unheard of even today, an example being the San Francisco light rail system, which caused error messages to appear on fare collection systems. A research study by **Embry-Riddle Aeronautical University [2]** also stated that rail control systems (like signals) are also potential targets for hackers. Data collected by the **Singapore Government [3]** also shows that as much as **3 million people** use the MRT **daily**, all of which would be affected if hackers attack the network.

Challenge #2:
Observation: During our interview with Prof. See, he stated that we may be overly dependent on AI. When this happens, the consequences of the automated system and AI malfunctioning would be more severe, as AI is given more and more control to free up the time fo humans.

Why this observation could pose a problem: This will be a problem as when we are too dependent on AI, a small failure in the system AI can cause widespread damage, be it to the safety of passengers or Singapore's economy as workers can be held up by MRT delays or disruptions. Inaccurate results collected by the AI could also mislead humans in charge of making decisions.

Research: A **Google AI** research paper **[4]** has stated the dangers of a malfunctioning AI, especially one in charge of an important task, like the management of a national metro system. AI may malfunction due to a multitude of reasons, some of which are inherent and out of human control.

According to an article by **Chron (A website about SMEs) [5]**, dangers in the overuse of technology in the workplace include loss of valuable files/documents if the technology fails, or malfunctions in valuable equipment causing property damage or loss of life.

Challenge #3:
Observation: During our interview with Prof. See, he stated that in the future, SMRT will have the need to process more data on its operations and therefore, will need to have a data centre for storing and processing of data.
SMRT generally collect data on what time do people tap into the station, what time they tap out, how much was spent as well as where are the stations with more traffic.

Why this observation could pose a problem: Without a proper security firewall, there could be a data breach and this stolen data can be dangerous to our social order.

Research: According to **ZDNet [6]**, which is a website on technology news, there has been a **data breach** of **Rail Europe**. The hackers possess data on **where and when** customers are going to board trains in Europe, which they then wait for the customers to tap into the station to **steal the credit** in their tickets. At the same time, **Singapore** had already experienced a **data breach** of **important personal data** during the **SingHealth cyberattack [7]**. This suggests that Singapore still has a ways to go in protecting citizens' data from being stolen.

Challenge #4:
Observation: During our interview with Mr Ng Wai Yi at SMRT HQ, he reflected that most, if not all, rail equipment will be automated and human-free. For instance, he raised the example of driverless trains, which are already in use locally today. Another, more futuristic example is the possible use of scanner equipped drones to monitor the condition of tracks. He also reflected that although there are in-built features that allow humans to take control if necessary, fewer and fewer human staff are bothering to learn how to operate such 'antiquated' technology, when a computer can run it for them.

Why this observation could pose a problem: Technology is not perfect, and is liable to failures. In the occasion where such a piece of technology fails, there is usually a human to take over, which reduces the efficiency by at most a fraction. However, in the Singapore of the future scene, where very few members of staff are trained to take over operation of such equipment, equipment failures will be much more drastic.

Research: According to a study by the **International Rail Journal**, technological trends in the industry point towards increasingly smart trains and driverless trains.

Challenge #5: During our interactions and Q&A sessions with SMRT staff from various departments, we discovered that the rail industry is quite lax towards cyberattacks, as many feel that they are not a 'key' target, like finance or healthcare. The closest SMRT has to a professional cybersecurity department is their 'Data Analytics' department, which is focused on the management of passenger and system data, and not cybersecurity.

Why this observation could pose a problem: With such a lax security attitude, SMRT will be caught unprepared in the case of an eventual cyberattack. If Singapore's rail network were to suffer a cyberattack, it would affect Singapore's economy in the way that many commuters cannot get to work on time, cause social disorder where many citizens feel insecure, etc.

Research: According to **The Local DK [8]**, a Danish news website, on 13 May 2018 there has been a cyberattack on **Danish state rail operator, DSB** and train passengers were prevented from buying tickets via the company's app, ticketing machine, website as well as unable to make any purchases in 7-Eleven stores in the stations. Ticket inspectors had to individually make sure that those with travel cards had tapped and at the same time sell tickets to keep the trains running, which they were not trained nor usually required to do. This caused much inconvenience and difficulty.

Group ID: 10-25

STEP 2. Craft the Underlying Problem

Using the challenges listed in Step 1, identify a problem of major importance to the chosen community / organization in the future. Write your Underlying Problem making sure your question clearly explains the action that will be taken and the desired results/goal of that action.

Incorporating Challenge(s) #1, 4, 5

Underlying Problem:

Given that technological advances have the potential to affect the safety and reliability of our public transport system by increasing its vulnerability to cyberattacks, while the public continues to underestimate and undermine such threats (Condition), how might we harden and protect our MRT system (KVP) such that the MRT continues to be a safe, efficient and reliable mass transport tool (Purpose) in the year 2030 and beyond? (FSP)

(EDIT TO IMPROVE)

Group ID: 10-25

STEP 3. Produce Solution Ideas

Generate solution ideas to the Underlying Problem in Step 2. Choose the 5 most effective solutions and write the elaborated ideas in the space provided. Include applicable research with appropriate in-text citations.

Solution #1:

We, the Infocomm Media Development Authority, will implement and enforce a national standard for cybersecurity. Like existing standards for carbon emissions and water saving, our cybersecurity standard will have different categories corresponding to different tiers of cybersecurity.

Higher tiers will have more stringent security requirements, which we recommend MRT trains and MRT infrastructure to be placed under. Such equipment has to pass strict testing, with white-hat hackers trying to breach the cyberdefenses of the abovementioned item.

If such a system is implemented, the Government can ensure that at least a basic standard of cybersecurity is implemented.

Solution #2:

We, SMRT, will organise regular cyber safety drills.

The drills will be conducted similar to fire drills, informing employees on the week the drill takes place, but not the exact day.

The drills will involve internal 'hackers' that try and breach the company/organisation's defenses, and attempt to wrest control of simulated targets, like trains and signals.

A reward scheme can then be used for the survivors of such 'attacks' to create more awareness of good cyber-security practices in the organisation, and further workshops/seminars can be held if it is determined that a certain method of cyberattack poses a great threat towards SMRT.

Solution #3:

We, SMRT will invest in training a trusted team of white-hat hackers to constantly test the security systems in place for the SMRT network.

They will do this by attempting to breach into SMRT systems and assets.

Any flaws/loopholes found will be reported to SMRT's cybersecurity division and patched.

This way, flaws and problems with the system can be found and patched, creating a security system that is constantly being updated to prevent hacking.

Solution #4:

We, the Land Transport Authority, will set up a programme to train commuters of the correct procedure in the event of a train disruption, whether caused due to technological faults or intentional acts.

Such commuters will be trained on how to react in such a situation, including the use of the emergency detrainment doors (doors at the front of the train) and the dos and don'ts in such a situation, and more

Commuters can sign up and participate in this programme for free, if they have logged a significant number of train trips in the past year, proving that they commute frequently.

This way, in the event of a train disruption, such 'trained commuters' would be able to assist their fellow passengers whom may be unaware of what to do, perhaps due to panic. This would reduce the impact on commuters, and by extension the impact on the system.

Solution #5:

We, SMRT, will send a fraction of our workforce for training in how to operate certain elements of the MRT network, like signal control or train driving. This will help harden our MRT network against cyberattacks, as there is a 'second layer of defense' preventing total failure of the system.

As it would be too expensive and too unrealistic to fully train every member of staff in every aspect of running a rail network, we will divide employees into groups and sort them into different trainings, accordingly. We will take this into account when deploying staff to MRT stations across the island, and we will ensure that each station has personnel capable of recovering from a situation.

Group ID: **10-25**

STEP 4a. Select Criteria

Generate criteria to determine which solution idea does the best job of solving your Underlying Problem and/or addressing the Future Scene situation. Select the 5 most important criteria for measuring solution ideas and write them in the spaces provided.

Criterion #1: Fastest to show effect

This is to judge which solution when implemented, shows immediate results and allow us to reap its benefits the earliest. This is not necessarily the fastest solution to implement, but the fastest solution to show effects.

Criterion #2: Easiest to implement

This is to judge which solution requires the least complicated procedures and time to implement, and thus allows (in a way) for decreased opportunity cost.

Criterion #3: Cheapest to implement

This is to judge which solution requires the least funds to implement, so as to reduce the financial losses on either SMRT, the government and/or other organisations involved.

Criterion #4: Benefits the commuters the most

This is to judge which solution when implemented and carried out, would not cause inconvenience to the commuters or cause the least inconveniences. Such inconveniences include but are not limited to; Early closing hours of stations, slower speed of trains, decreased frequency of trains etc.

Criterion #5: Most future-proof

This is to judge which solution is the most flexible, so that when other issues and challenges pop up in the future, said solutions can be change and adapt to solve the challenges.

STEP 4b. Apply Criteria

List the solution ideas from Step 3 on the grid. Use each criterion to rank the solutions on a scale from 1 (poorest) to 5 (best). The weighting for one important criterion may be doubled if necessary.

Step 3 Sol'n #	Solution Idea	Criteria					Total
		1	2	3	4	5	
#1	Implement a national standard for cybersecurity	1	2	3	4	5	15
#2	Conduct cyber safety drills	5	3	2	1	4	15
#3	Training a trusted team of white hackers	3	1	1	4	4	14
#4	Programme for train commuters to learn what to do in case of emergency	5	2	3	5	5	20
#5	Training all staff to operate certain elements of SMRT rail network	1	3	3	4	4	15

STEP 5. Develop an Action Plan and Evaluate its Feasibility

Develop your top-scoring solution idea into an Action Plan. Thoroughly explain how the Underlying Problem is solved, how the plan will be implemented, and how the community / organisation will be affected. Explain how this Action Plan is feasible with secondary research consulted, preferably also with primary research (feedback from chosen community / organization)

Action plan derived from Solution 4:

We, the **Land Transport Authority**, will work together with the **Public Transport Council**, **SMRT**, and **SBSTransit**, to develop a workshop to prepare commuters in the event of a rail emergency. Such emergencies can range from a simple train disruption to a network-wide cyberattack leading to failure of key systems.

During this 1-day workshop, participants will learn about the Dos and Don'ts in such a situation, and will learn a standard protocol for responding. They will also be advised to assist other passengers, especially the elderly and infirm, or those with young children. Practical aspects of the workshop include how to operate the detrainment doors (the emergency doors at the front and back of the train), and how to use the manual door controls in the trains (in event of a power failure).

Commuters who have been identified as frequent travellers (use the MRT 5/7 days of the week) will be invited to join this workshop, which will be free of charge. Their contact details will be collected such that SMRT and SBSTransit can keep them informed in the event of any situation.

Technology will be heavily utilised in this workshop, especially VR and AR simulations.

Smartphones also play an integral part of this programme, as commuters will be contacted of what to do in the case of any incident, even if they are not directly affected.

This action plan is similar to Singapore's present anti-terrorism drills, like Operation Northstar or Exercise Heartbeat, where members of the public are trained in life saving skills like CPR. However, this workshop will be much more specialised and tailored to rail commuters. We will also recommend that small discounts on train rides be given to those who have attended the workshop and are certified to have passed the workshop.

In our meetings with SMRT staff, we have discussed and proposed this idea to members of different departments. However, it requires a large amount of logistical effort, as multiple departments and multiple organisations have to be involved. For example, the abovementioned Exercise Heartbeat required participants ranging from Changi Airport to the Ministry of Health.

However, if this programme is a success, cyberterrorists will note our MRT system has a 'hardened target' and will learn that their attacks do not do much damage to a well-prepared and well-drilled community.

Bibliography

Cite the resources you consulted using the APA format.

List of References:

PTC: Public Transport Council. (n.d.). Retrieved June 6, 2019, from https://www.ptc.gov.sg/

SMRT: Our Businesses. (n.d.). Retrieved June 6, 2019, from https://www.smrt.com.sg/

SMRT-NTU Smart Urban Rail Corp Lab: NTU Smart Urban Rail Corporate Lab. (n.d.). Retrieved June 9, 2019, from https://smrt-ntu-smarturbanrail.ntu.edu.sg/Pages/index.aspx

LTMP: LAND TRANSPORT MASTER PLAN (LTMP) 2040. (n.d.). Retrieved June 19, 2019, from https://www.lta.gov.sg/content/ltaweb/en/about-lta/what-we-do/ltmp2040.html

Antony, A. (2019, March 05). How will AI impact the transportation industry? -Prescouter - Custom Intelligence, On-Demand. Retrieved March 31, 2019, from https://www.prescouter.com/2017/12/ai-impact-transportation-industry/

Benefits of Artificial Intelligence in the Transportation Industry | Infiniti Research. (2018, June 19). Retrieved March 31, 2019, from https://www.infinitiresearch.com/thoughts/ai-transportation-industry

The 25 Ways AI Can Revolutionize Transportation: From Driverless Trains to Smart Tracks. (2018, May 02). Retrieved March 31, 2019, from https://interestingengineering.com/the-25-ways-ai-can-revolutionize-transportation-from-driverless-trains-to-smart-tracks

[1] Liptak, A. (2016, November 28). Hackers are holding San Francisco's MUNI light-rail system for ransom. Retrieved June 22, 2019, from https://www.cnbc.com/2016/11/28/hackers-are-holding-san-franciscos-muni-light-rail-system-for-ransom.html

[2] Szechy, A. (n.d.). Transportation Hacking. Retrieved June 22, 2019, from http://pages.erau.edu/~andrewsa/Project 3/Szechy_Adam/hacking_ams.html

[3] Public Transport Utilisation - Average Daily Public Transport Ridership. (n.d.). Retrieved July 22, 2019, from https://data.gov.sg/dataset/public-transport-utilisation-average-public-transport-ridership?view_id=3619b55d-d1c2-4891-8b43-97b192bcb0c4&resource_id=552b8662-3cbc-48c0-9fbb-abdc07fb377a

[4] Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., & Mané, D. (2016, Spring). Concrete Problems in AI Safety. Retrieved July 26, 2019, from https://ai.google/research/pubs/pub45512

[5] Joseph, C. (2017, November 21). The Disadvantages of Computers in the Workforce. Retrieved June 26, 2019, from https://smallbusiness.chron.com/disadvantages-computers-workforce-10004.html

[6] Whittaker, Z. (2019, January 18). Rail Europe had a three-month long credit card breach. Retrieved June 24, 2019, from https://www.zdnet.com/article/rail-europe-had-a-three-month-long-credit-card-breach/

[7] Kwang, K. (2018, October 18). Singapore health system hit by 'most serious breach of personal data' in cyberattack; PM Lee's data targeted. Retrieved June 24, 2019, from https://www.channelnewsasia.com/news/singapore/singhealth-health-system-hit-serious-cyberattack-pm-lee-target-10548318

[8] Local, R. (2018, May 14). Cyber attack hits Danish rail network. Retrieved June 30, 2019, from https://www.thelocal.dk/20180514/cyber-attack-hits-danish-rail-network