**RMPP Unit 10 Presentation Transcript**

*Instructions: To view the presentation recording, set the PowerPoint presentation to presentation mode on the title slide.*

Hello, my name is Freya Basey and this presentation covers a research proposal for Applying a Cyber Incident Response and Recovery Framework to Intelligent Transportation Systems using Nissan as a case study.

A key area of current technological development is Intelligent Transportation Systems (ITS), with road-based ITS being a particular area of interest due to the increasing challenges seen in urban road systems (Vitunskaite et al., 2019). Road-based ITS forms a cornerstone of the smart city concept and aims to improve urban living through reducing travel times, emissions and congestion (Chen et al., 2018). The ITS literature shows a lean towards the connected and autonomous vehicles (CAV) use case and this is likely due to the significant ongoing investment in this technology, with almost two thirds of mobility investments going towards autonomous vehicles and smart mobility since 2010 (Holland-Letz et al., 2021).

Previous research shows that ITS infrastructure, from cars to traffic signals, could be vulnerable to both existing and yet to be discovered cyber threats (Chen et al., 2018). When it comes to the security of ITS, the literature makes clear the importance of resilience in order to protect against these threats (Vivek & Conner, 2022; Ganin et al., 2019). However, whilst there has been various studies focusing on security controls, there has been little focus on cyber recovery in the event of an impactful cyber attack. The significance of this project lies in the fact that recovery is a key cyber security control function that needs to be understood and addressed in order to protect a system from inevitable cyber attacks (NIST, 2018; NIST, 2021). It is on this basis that this project would meet the requirement for the Master of Science (MSc) Cyber Security course. With regards to the scope of this study, it is proposed that the focus will be system recovery from active cyber attacks in road-based ITS (Husnoo et al., 2021).

In order to address the identified research gap, the aims of this study will be to provide insight into how cyber recovery controls can be applied to ITS use cases as well as the current state of recovery controls in the industry. Furthermore, the study will seek to identify opportunities, challenges and gaps regarding cyber recovery in ITS.

The following research questions will be used as a basis for the study in order to achieve these aims:

* Is the Cyber Incident Response and Recovery Framework applicable to road-based ITS (Staves et al., 2022)? If not, how could it be adapted to suit this use case?
* Which cyber recovery controls are applicable to the road-based ITS use case?
* What gaps and challenges are there in current ITS recovery controls?

In order to answer the research questions, the underlying objectives will include:

* Apply an existing cyber recovery framework to the Nissan autonomous vehicle use case and determine if any adaptations are required.
* Identify which cyber recovery controls are in use or could be applied to the use case.
* Identify opportunities for valuable future research and development.

Based on previous research, my initial hypotheses would be that the framework is largely applicable to the ITS use case with some omissions and gaps. Whilst recovery controls are important for ITS, I would expect them to still be maturing due to the infancy of the technology. Furthermore, emergency situations and privacy requirements inherent in ITS may add some complexities not covered in the Industrial Control Systems (ICS) application of the framework (Staves et al., 2022).

This project would take the form of a theoretical application of an existing framework so would be both descriptive and exploratory in nature (Dawson, 2015). The proposed research methodology to achieve the objectives of the project is a case study, from both an indirect and direct perspective. Indirect through applying the framework to several ITS attack scenarios based on secondary Nissan data that is publicly available and direct through a confirmatory round of interviews with stakeholders involved in Nissan cyber recovery activities. Whilst case studies are not always reliable for descriptive research due to the risk of atypical respondents, using multiple sources will allow me to better determine the probable truth and will allow for considered generalisations based on the outcomes of the study.

Research design should follow a recognised process (Dawson, 2015). Whilst a sequential process has been defined for this project, some of the stages will be iterative in nature, such as the data analysis and framework application stages.

The first step will be to identify attack scenarios that are applicable to the Nissan case study based on publicly available data, some of which is covered in the next slide. The initial intention is to identify two attack scenarios and then simulate the attacks to ensure that they are both viable and fully understood. A simulation is chosen here due to the lack of available real-world testbeds and also out of caution regarding any potential contraventions of the Computer Misuse Act 1990 (Ahmadi-Assalemi et al., 2020; CPS, 2020).

The second step will be applying the Cyber Incident Response and Recovery Framework to the attack scenarios for the Nissan case study, again based on secondary data, to understand how the framework would be utilized. Using more than one attack scenario will allow for comparison and contrasting to fully understand the framework’s applicability and how cyber recovery controls can be leveraged for CAV, and ultimately for ITS.

The third step is interviewing Nissan stakeholders involved in cyber operations to confirm and potentially expand on the findings of the framework application. Whilst observations could lead to a rich view of the cyber recovery process, the logistics for organising this as well as the highly sensitive nature of cyber security incidents make this data collection method unsuitable (Staves et al., 2022). Instead, the intention is to follow the original application of the framework in using semi-structured interviews. Semi-structured interviews are appropriate here as some structure will ensure focus on the coverage of the key framework elements whilst allowing flexibility to probe further on areas of interest and confirm meanings if required. In order to avoid biased answers, questions exploring the current approaches to each section of the framework will be asked prior to sharing the framework itself. Following that, the framework will be explicitly shared with interviewees to understand their views on the suitability of the framework in its entirety.

The fourth step will be to aggregate and analyse the qualitative data gathered during both the framework application and subsequent confirmatory interviews. Given the qualitative nature of the data, content analysis will be used to determine key themes and ideas. Particular attention will be paid to whether the data from the application of the framework aligns with interview responses and consider why this may or may not be. Whilst the reliability of qualitative methods is often weaker than quantitative designs, validity is often stronger due to the rich data observed and the resulting interpretations (Kaplan & Maxwell, 2005).

The final step will be to document findings on the framework suitability, including challenges and gaps. When it comes to organising and documenting the findings of the study, the IMRAD structure will be used (Anderson & Hepburn, 2020; Wu, 2011). The IMRAD structure uses the core sections of introduction, methods, results and discussion. The simplicity of this foundational structure means that additional sections can be added to enhance communication of the study, for example by adding a conclusion and suggestions for future research.

Several resource requirements are clear from the outset of this study. These include attack simulation software to test potential attack scenarios, means of efficiently making both voice and note recordings during interview, and access to suitable Nissan stakeholders. Initial research demonstrates that there is open-source software available to support attack simulations (SUMO, 2022), a smart device could be used for both recordings, and finally I can leverage my professional network to access Nissan stakeholders.

Another resource required to conduct research is existing literature applicable to the study (Dawson, 2015). There are several topics to consider when identifying key literature related to this project, for example the case study itself, ITS resilience and cyber recovery. The following are some examples of current sources that will be used to support and inform the direction of the project.

Given the chosen research approach, confirmation that there is sufficient secondary data available on the Nissan autonomous vehicle case study is key. Fortunately, there are several resources available from Nissan, including regular press releases and articles discussing technological innovations. Nissan (2017) covers the vision, core capabilities and real-world trials of the autonomous vehicle use case. Nissan (2020) and Partridge (2020) go on to discuss the successful trials Nissan has run in the UK. UKR&I (2022) and Nissan (2022) provide context regarding ongoing ServCity trials being led by Nissan along with details of key stakeholders that may be useful for identifying interviewees. Finally, Nissan (N.D.a) and Nissan (N.D.b) provide insights into both existing technologies utilised in trials as well as future direction; both insights will likely come in handy for identifying attacks relevant to the Nissan case study.

Whilst cyber recovery has not been covered in detail for the road-based ITS use case, there has been research into cyber resilience in ITS. Vivek & Conner (2022) discuss the importance of resilience in ITS given the associated threats and vulnerabilities. Both Vivek & Conner (2022) and Ganin et al. (2019) cover attack simulations which can be used to identify relevant technologies and techniques to support the attack definitions in the proposed study. In addition, Ganin et al. (2019) considers the idea of component criticality and acknowledges the importance of resilience in the face of unknown threats due to the limited deployment of large-scale ITS to date. Ahmadi-Assalemi et al. (2020) highlights gaps in the security research around smart cities, including lack of consideration for digital forensic incident response and a lack of available datasets for testing. Overall, this shows that the gap could be even wider than ITS and due consideration should be given to the datasets used for attack definition.

When it comes to cyber recovery, Staves et al. (2022) and Lancaster University (N.D.) define the Cyber Incident Response and Recovery Framework. This is designed for critical national infrastructure, such as transportation systems, so is the framework that has been chosen for application in this study. Clark et al. (2018) provides inspiration in the form of cyber recovery strategies applied in another ITS use case, namely aviation. Onwubiko (2020) not only provides an alternative cyber recovery framework based on NIST guidance but also acknowledges the cyber recovery research gap and the importance of research in this area. Furthermore, Bartock et al. (2016) is a NIST special publication on cyber event recovery that can be leveraged during this study. Guidance from the NCSC Cyber Assessment Framework will also be useful when considering the possible opportunities, challenges and gaps in applying the Cyber Incident Response and Recovery Framework.

Ethics must be considered when performing research and ethical approval must be given by the university prior to carrying out primary research (Dawson, 2015; University of Essex Online, 2020). Public expectations of ethical practice is increasing, including with regards to research (Vanclay et al., 2013), and an ethical approach can support the integrity of the study (Miller et al., 2012).

Using human subjects as part of this study adds some additional considerations when it comes to ethics (Vanclay et al., 2013). For example, any participants must be informed about how their data will be used and give consent based on those uses. Also, I will need to avoid collecting any unnecessary personal data, limiting the data to demographic only for example (Staves et al., 2022). Any personal data collected will need to be protected due to the participant’s right to privacy and the associated regulatory requirements, such as the General Data Protection Regulation (GDPR) (EUR-Lex, 2016). The GDPR stipulates that a reasonable retention period should be set to determine how long data is kept for and the data must be securely stored for the duration of that time. In addition, using an organization as a case study and gathering primary data related to the organization may require suitable confidentiality agreements to be in place.

Further to ethical considerations in how the data is collected and processed, there are ethical considerations regarding presenting results too (Dawson, 2015). As a professional in IT, I have a responsibility to act with integrity and competence which involves ensuring any results are objective; using all results from the study to ensure accuracy and prevent bias (BCS, 2021). It is worth noting that, although ethical challenges can be identified from the outset of the project, ethical considerations should be included throughout the research lifecycle and form part of the overarching risk assessment process for the project (Miller et al., 2012).

Risks to be considered include those that threaten the successful completion of the project. These can include lack of access to required resources, limited timelines to complete the project in, and even validity issues, such as biased results where Nissan stakeholders want to avoid exposing gaps in their cyber recovery approach for example (Dawson, 2015). The key to managing these risks is identifying and managing them as soon as possible. For example, the aforementioned risks could be managed with appropriate planning of both resources and timelines as well as employing best practice research techniques, such as building trust with interviewees and avoiding leading questions (Staves et al., 2022). Finally, one of the key risks to this research design would be if permission to interview Nissan stakeholders is withheld by the company. Contingencies could include utilizing another organization as the case study, for example Oxbotica (Oxbotica, 2022), or adapting the confirmatory step to not be so heavily focused on the particular case study. Overall, risks management will be a continuous process in the lifecycle of this project.

This timeline is based on the planned upcoming MSc Project Module running for 30 weeks from Tuesday 3rd May 2022. Some steps of the study must run concurrently, for example simulation testing of the attack scenarios must be concluded before beginning to apply the framework to the scenarios, however others can run in parallel, for example documentation of findings can begin whilst analysis work is still ongoing. Based on experience of managing professional projects, I have been generous with the time assigned to each stage to allow for any challenges to be resolved, for example August is a popular time for holidays abroad for those with children so allowing four weeks to conduct interviews should mitigate the risk of interviewees not having availability.

In this research proposal, a five-stage research design has been proposed in order to fill a gap identified in current cyber security research. Whilst there will be no artefact developed, addressing the research problem via these steps will contribute knowledge regarding the current state of cyber recovery controls in Intelligent Transportation Systems. This includes sharing actionable information that would benefit ITS operators and academics with regards to current cyber recovery knowledge. Understanding cyber recovery is significant in this context as these controls will be core to ensuring and promoting the overall resilience of these systems in order to preserve their critical functions, including public safety. Research into new areas can be challenging, especially with the target technology in its infancy, and potential project challenges have been identified. Intended solutions and contingencies have been covered, but the risk management process will be important throughout the project as unforeseen challenges inevitably emerge. Overall, this is a viable project that could pave the way for future research in this area and support the fast-paced innovation in the smart mobility sector.

References

Ahmadi-Assalemi, G., Al-Khateeb, H., Epiphaniou, G. & Maple, C. (2020) Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review. *Smart Cities* 3(3): 894-927.

Anderson, H. & Hepburn, B. (2020) 'Scientific Method' in: Zalta, E. (eds) *The Stanford Encyclopedia of Philosophy* (Winter 2020 edition). Metaphysics Research Lab, Stanford University.

Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G. & Scarfone, K. (2016) NIST Special Publication 800-184: Guide for Cybersecurity Event Recovery. Available from: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf> [Accessed 27 March 2022].

BCS (2021) Code of Conduct for BCS Members. Available from: <https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf> [Accessed 27 March 2022].

Chen, Q., Sowan, A. & Xu, S. (2018) ‘A safety and security architecture for reducing accidents in intelligent transportation systems’, *Proceedings of the International Conference on Computer-Aided Design*. San Diego, California, 5-8 November. New York, USA: Association for Computing Machiner. 1–7.

Clark, K., Bhatia, U., Kodra, E. & Ganguly, A. (2018) Resilience of the U.S. National Airspace System Airport Network. *IEEE Transactions on Intelligent Transportation Systems* 19(12): 3785-3794.

CPS (2020) Computer Misuse Act. Available from: <https://www.cps.gov.uk/legal-guidance/computer-misuse-act> [Accessed 27 March 2022].

Dawson, C. (2015) *Projects in Computing and Information Systems: A Student's Guide*. Harlow: Pearson.

EUR-Lex (2016) REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Available from: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [Accessed 27 March 2022].

Ganin, A., Mersky, A., Jin, A., Kitsak, M., Keisler, J. & Linkov, I. (2019) Resilience in Intelligent Transportation Systems (ITS). *Transportation Research Part C: Emerging Technologies* 100: 318–329.

Holland-Letz, D., Kässer, M., Kloss, B. & Müller, T. (2021) Mobility’s future: An investment reality check. Available from: <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/mobilitys-future-an-investment-reality-check> [Accessed 28 March 2022].

Husnoo, M., Anwar, A., Chakrabortty, R., Doss, R. & Ryan, M. (2021) Differential Privacy for IoT-Enabled Critical Infrastructure: A Comprehensive Survey. *IEEE Access* 9:153276–153304.

Kaplan, B. & Maxwell, J. (2005) ‘Qualitative Research Methods for Evaluating Computer Information Systems’, in: Anderson J. & Aydin C. (eds) *Evaluating the Organizational Impact of Healthcare Information Systems*. New York: Springer. 30-55.

Lancaster University (N.D.) ICS Response & Recovery Framework. Available from: <https://ics-rr-framework.github.io/> [Accessed 27 March 2022].

Miller, T., Birch, M., Mauthner, M. & Jessop, J. (2012) *Ethics in Qualitative Research*. 2nd ed. London: SAGE.

NCSC (N.D.) D.1 Response and recovery planning. Available from: <https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/d-1-response-and-recovery-planning> [Accessed 27 March 2022].

Nissan (2017) Nissan conducts on-road autonomous vehicle testing in Europe. Available from: <https://uk.nissannews.com/en-GB/releases/release-426183293-nissan-conducts-on-road-autonomous-vehicle-testing-in-europe> [Accessed 27 March 2022].

Nissan (2020) Nissan LEAF completes the UK's longest and most complex autonomous car journey. Available from: <https://uk.nissannews.com/en-GB/releases/release-d6f92ce01d194b464003d8e64c0103e6-nissan-leaf-completes-the-uks-longest-and-most-complex-autonomous-car-journey> [Accessed 27 March 2022].

Nissan (2022) ServCity: a project making autonomous mobility a reality in the UK’s cities. Available from: <https://europe.nissannews.com/en-GB/releases/release-832261c25e9d6fa480b83b275d47b334-servcity-a-project-making-autonomous-mobility-a-reality-in-the-uks-cities> [Accessed 27 March 2022].

Nissan (N.D.a) Philosophy of Nissan autonomous drive technology development. Available from: <https://www.nissan-global.com/EN/TECHNOLOGY/OVERVIEW/autonomous_drive.html> [Accessed 27 March 2022].

Nissan (N.D.b) Seamless Autonomous Mobility: The Ultimate Nissan Intelligent Integration. Available from: <https://www.nissan-global.com/EN/TECHNOLOGY/OVERVIEW/sam.html> [Accessed 27 March 2022].

NIST (2018) Framework for Improving Critical Infrastructure Cybersecurity. Available from: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> [Accessed 27 March 2022].

NIST (2021) The Five Functions. Available from: <https://www.nist.gov/cyberframework/online-learning/five-functions> [Accessed 28 March 2022].

Onwubiko, C. (2020) ‘Focusing on the Recovery Aspects of Cyber Resilience’, *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. Dublin, Ireland, 15-19 June. IEEE. 1-13.

Oxbotica (2022) Our Company. Available from: <https://www.oxbotica.com/our-company/> [Accessed 30 March 2022].

Partridge, J. (Feb 5, 2020) Nissan Leaf breaks UK record for longest self-driving car journey. *The Guardian*. Available from: <https://www.theguardian.com/business/2020/feb/05/nissan-self-driving-car-leaf-longest-journey> [Accessed 27 March 2022].

Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A. & Hutchison, D. (2022) A Cyber Incident Response and Recovery Framework to Support Operators of Industrial Control Systems. *International Journal of Critical Infrastructure Protection* 37.

SUMO (2022) Simulation of Urban Mobility. Available from: <https://www.eclipse.org/sumo/> [Accessed 27 March 2022].

UKR&I (2022) ServCity. Available from: <https://gtr.ukri.org/projects?ref=105091> [Accessed 27 March 2022].

University of Essex Online (2020) Academic Offences Procedures 2020-21. Available from: <https://online.essex.ac.uk/wp-content/uploads/Legal-Documents/Academic-Offences-Procedures.pdf> [Accessed 27 March 2022].

Vanclay, F., Baines, J. & Taylor C. (2013) Principles for ethical research involving humans: ethical professional practice in impact assessment Part I. *Impact Assessment and Project Appraisal* 31(4): 243-253.

Vitunskaite, M., He, Y., Brandstetter, T. & Janicke, H. (2019) Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security* 83: 313–331.

Vivek, S. & Conner, H. (2022) Urban road network vulnerability and resilience to large-scale attacks. *Safety Science* 147: 105575.

Wu, J. (2011) Improving the writing of research papers: IMRAD and beyond. *Landscape Ecology*26: 1345–1349.