A Review of Resilience in Autonomous Transport to Improve Safety and Security

S. O. Johnsen and S. S. Kilskar
SINTEF, Trondheim, Norway. E-mail: Stig.O.Johnsen@sintef.no

The risks of autonomous systems are emerging and we need to explore how risks can be mitigated through resilience engineering. This paper presents results from a literature review on resilience in autonomous transport systems (i.e. resilience, autonomy, transport) aiming to answer: How can resilience be used to improve safety and security of autonomous transport systems? What can the various transport modes learn from each other regarding resilience and autonomy; and more specifically, what issues are of interest for the maritime sector? The results show that resilience has been identified as an important enabler for safety and security of autonomous systems, with increased attention from 2017. Many of the papers discuss resilience in the context of safety improvements, or resilience against system failures. Most of the literature covers autonomy in road traffic and aviation. Findings from these modes can provide input to design and enhance resilience of maritime autonomy. As an example, the importance and resilience of infrastructure (i.e. intelligent infrastructure support) supporting autonomy in aviation and road traffic may be explored in improving resilience of maritime autonomy. The breadth of security issues from road transportation should be explored in the maritime industry. More exploration of existing research is needed in the maritime sector to select and build upon existing research from the other modes.

Keywords: Autonomy, transport systems, resilience, safety, security.

1. Introduction

1.1 *Background and motivation*

Automated transport vehicles are being deployed in several transport modes (i.e. road, rail sea, air), with different levels of autonomy (LoA) and different levels of maturity. Automation has usually been implemented to perform dirty, dull, dangerous or demanding operations, and/or to remove humans from danger. Reliability, safety and security of autonomous transport systems are key requirements for the use and acceptance of these systems. The experiences and risks of automated transport systems are emerging. The predominant engineering perspective has been to automate as much as possible, and to minimize human interactions. A balanced integration between meaningful human control, human factors and technology has often been missing (Cummings, 2014), leading to poor reliability.

As an example, in Petritoli et al. (2017) the Main Time Between Failures (MTBF) was estimated for automated aviation systems (drones), to be 1000 hours. This is approximately 100 times poorer than MTBF in manned flights, where MTBF are 100 000 hours. The mishap rate of remotely operated drones is significantly higher than manned operations. Rate of incidents in drone operations are 50-100 mishaps for every 100,000 flight hours' vs human-operated aircraft where there is one mishap per 100,000 flight hours. Main causes are related to poor attention to human factors science, such as poor design of ground control systems (Waraich et al., 2013; Hobbes et al., 2014). The need for handling these higher rate of failures and mishaps, are important in automated systems. Our scope is the automated systems in the defined operational domain, the "drone", communication to control facilities and to needed infrastructure.

Pre-programmed systems are challenged when the unanticipated is happening, thus resilience as the ability to handle the unanticipated, is one key factor in automation. However, resilience has seldom been included. A report on resilience in transportation concludes that one of the primary challenges is a lack of clear perception of resilience engineering methods and how resilience and safety can affect each other National Academies of Sciences (2018). Thus, there is a need to explore how reliability, safety and security can be supported in autonomous systems through resilience engineering.

This paper presents the results from a literature review on resilience in autonomous transport systems. We have performed this review in order to identify relevant knowledge (i.e. peer reviewed publications of resilience in the area); list recent major advances or debates; and identify gaps in the research. This review paper aims to answer the following questions:

1) How can the resilience perspective be used to improve safety and security of autonomous transport systems?

2) What can the various transport modes learn from each other regarding resilience and autonomy; and more specifically, what issues are of key interest for the maritime sector?

Proceedings of the 30th European Safety and Reliability Conference and
the 15th Probabilistic Safety Assessment and Management Conference.
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
 Published by Research Publishing, Singapore
ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0 esrel2020psam15-paper

1.2 *Definitions and central concepts*

In the following we have defined some key terms and concepts.

In Parasuman and Riley (1997) automation is described as "*The execution by a machine agent (usually a computer) of a function that was previously carried out by a human*. In SAE (2016) there is a definition of levels of automation (LoA), going from no automation to full autonomy in six steps. Autonomy and automated is often not clearly defined, used or delineated. By *autonomy* we mean a system that is non-deterministic in that it has a freedom to make choices, and by *automated* we mean a system that is more deterministic in that it will do exactly what it is programmed to do. This definition is somewhat based on the taxonomy and discussion of automation from Vagia et al. (2016).

One of the challenges of automation is the ability to handle the unanticipated, changes or disturbances. The ability to be resilient, is an important property in this context. Resilience (RE) is here defined as "*the intrinsic ability of a system to adjust its functioning prior to or following changes and disturbances, so that it can sustain operations even after a major mishap or in the presence of continuous stress*" (Hollnagel, Woods and Leveson, 2006). Key taxonomies are based on Avizienis et al (2004). The paper is structured in the following sections:

- This introduction
- Description of methods and approach
- Results
- Conclusions and further research
- Appendix with overview of publications

2. Method and approach in review

A literature review was conducted to establish a knowledge base on resilience in autonomous transport systems, with search strings in Table 1.

Table 1. Search strings

Database	Search string
Scopus	TITLE-ABS-KEY ((autonom* OR automat*) AND resilien* AND (transport* OR vehicle)
Web of Science	TOPIC: ((autonom* OR automat*) AND resilien* AND (transport* OR vehicle)

Boolean searches were carried out in the interdisciplinary databases Scopus and Web of Science with the aim to cover combinations of variations of the terms *autonomous*, *resilience* and *transport*. In addition to the term *autonomous*, publications using variations of the term *automated* may also be of interest; thus, we included this search term. In the papers, there has not been any clear distinction between the terms *autonomous* and the term *automated*. Using an asterisk (*) on the applied search terms, variations of the terms were returned. Examples of these variations are listed in Table 2.

Table 2. Variations of the search terms

Search term	Variations of the term (examples)
autonom*	autonomous, autonomy
automat*	automation, automated, automatic
resilien*	resilience, resilient, resiliency, resiliently
transport*	transport, transportation

The searches were limited to the ten-year-period 2010-2019, and only publications in English were included for further review.

As aspects of safety and security may be discussed using different terms (e.g. attacks, accidents), no requirement regarding the inclusion of 'safety' and/or 'security' was made. However, articles and papers that do not discuss resilience in relation to aspects of safety and/or security were excluded for further review. So were articles and papers briefly mentioning 'resilience' without actively using the concept.

3. Results

The literature search resulted in a total of 50 publications that were included for further review. See Table A1 in the appendix for a chronologically listed overview of the included publications. The list includes 20 articles published in peer-reviewed scientific journals and 30 papers presented at international conferences.

The number of papers has increased significantly from 2017. We found 1 paper in 2010; 1 in 2011; 1 in 2013; 4 in 2014; 2 in 2016; 12 in 2017; 11 in 2018 and 18 in 2019.

Most of the papers focused on specific transport modes, but some covered all modes:

- All modes: 6 papers
- Road: 25 papers
- Air: 10 papers
- Sea: 7 papers
- Metro/Rail: 2 papers

Resilience is the key concept in the papers, but has been based on different definitions. We have structured the papers in areas, such as resilience in design of the systems (or scope of use i.e. operational design domain to support resilience), resilience built by testing or learning and resilience in operations (based on control systems, infrastructure or to handle security).

Automation in (commercial) aviation and automation metro/rail have impressive safety records but no papers have discussed resilience in these modes.

3.1 *Papers covering all modes*

To summarise the papers, there are challenges with autonomy and there is a need to explore resilience in design of autonomous systems; resilience of control systems and the importance of resilience to handle security issues.

Resilient Design: Vachtsevanos et al (2018) say that autonomous systems are proliferating and their utility are increasing. The development of resiliency and safety is not keeping pace with their growth rate. Several factors impede their adoption: the absence of reliable autonomy; challenges in human-machine interface; the need for emerging machine learning and resilience to assure safety; reliability when executing missions in unstructured environments. A resilient system is monitoring its internal and external environment, it can detect and anticipate disturbances and take appropriate actions to ensure operations within a safety envelope. The paper introduces a framework for resilience of such systems via self-organization and control reconfiguration strategies. It further introduces fault-tolerance by giving input to a reinforcement learning strategy. In Wied et al (2018) resilient design properties of a driverless transport system are described. They study resilient properties and classify them by function into six distinct categories, to be used to ensure resilient design. In Zieba et al (2010), they describe principles of adjustable autonomy to ensure resilient human–machine cooperation. To be efficient, the human–robot system must be able to anticipate, react and recover from errors of different kinds, i.e., to be resilient. The paper proposes three indicators to assess different meanings of resilience of the system: foresight and avoidance of events, reaction to events and recovery from occurrence of events. Zieba et al (2011) focus on autonomous systems performing missions of surveillance, under the remote supervision of human operators. Operations are likely to face perturbations in a dynamic environment, that challenges the human operators due to overload. The objective of this study is to improve resilience so that it can better manage perturbations, by making the level of autonomy adjustable. The results were analysed using: efficiency, adaptability, border-line functioning and interaction. The data showed that the effect of cooperative control depends on the nature of the perturbations; as an example, perturbations that require the intervention of the human operator to assist the system are more difficult for the operators to manage.

Resilience in control systems (Graphs): Bucic et al (2019) describe work with a theoretical, graph-based method for an autonomous system to be able to achieve its control objective even if the system partially loses control authority. They obtain conditions for existence and an efficient algorithm for determining design and control policy that preserve system safety. The next goal is to provide a simple graph-based criterion for existence of a system design that admits a correct control policy. Such a method would be a step towards ensuring system resilience under partial loss of control authority.

Resilience to handle security challenges: Ray (2017) gives an overview of security challenges and need for resilience in Transportation, especially Highways and Roads, with a focus on security challenges, interaction of infrastructure, transporting agents, and vehicle communication.

3.2 *Road*

To summarise the papers, resilience should help improve trust; resilience must include supporting infrastructure and are important to mitigate security issues/ unanticipated issues; resilience must be a part of architecture/ early design and design of redundancy is important; resilience of control system has been in focus especially to handle security issues (i.e. denial of service,..); resilience could be a part of transition from LoA; and prioritize testing of resilience.

Trust: In Henschke (2019), the role of trust in the development of resilient autonomous driving systems is discussed. It is pointed out that in order to have autonomous systems that are worthy of our trust, we need a structure of oversight and a process that designs trust into the systems from the outset. The systems have risks, but we need resilient systems that can survive accidents and tragedies, and learn and improve from them.

Resilience in transport operation: An analysis of road transportation resilience was given in Ahmed et al (2019), showing that the resilience of the transportation system improved with automated systems and intelligent infrastructure support (ITS) in relation to travel time and capacity improvement. In Ganin et al (2019), they explore the implications for transportation resilience when ITS systems become prevalent. They argue that network science provides a foundation for the evaluation of trade-offs in designing smart and resilient transportation systems. The authors have analysed directed and random attacks on node and link disruptions in urban transportation networks. Understanding transportation network resilience is important for several reasons. Resilience can support how well a system is able to perform during failures. Poor performance could be improved with ITS investments. Resilience can also be used to plan for unknowable events and vulnerabilities, which traditional risk frameworks cannot. They contribute by providing a method and metric to assess ITS road network resilience and by performing a case study of the method for

10 cities. In Khan et al (2016) they discuss how to enhance resilience of transportation systems. Resilience is defined as the ability to resist the loss of traffic-serving capability by using road design (e.g. with flexibility to accommodate random traffic overloads) and control system design (i.e. activating capacity-enhancing measures to ensure dynamic resilience). The goal is to enhance the resilience of urban traffic to withstand imbalances of demand vs. capacity as well as stochastic traffic overloads and recover within acceptable time.

Resilient Architecture: Techniques and ideas for applying resilience to system-of-systems (SoS) of autonomous military vehicles is explored by Klingensmith and Madni (2017). The paper describes resilience techniques to enable a system to face disruptions and continue operating. In Madni et al (2017a), they present a model-based approach for engineering resilient SoS called the resilience contract (RC). Ratasich et al (2019) summarize the state of the art of existing work on anomaly detection, fault-tolerance, and self-healing, and add a number of methods applicable to achieve resilience in a general Internet of Thing context, presenting the main challenges in building a resilient control system/ cyber physical system such as connected autonomous vehicles.

Resilience by redundancy: In Ängskog et al (2018), the need for resilience was highlighted since vehicles and the intelligent transport system infrastructure must be able to handle natural disturbances and attacks of malicious nature-proposing a shift toward resilience engineering and vulnerability analysis to manage antagonistic threats. The positioning system (GNSS) needs to be resilient by using redundant information such as inertial navigation and dead reckoning. Redundancy is used in Bezzo et al (2014); describing a methodology to control ground robots under attack on sensors. They use a control-level technique using redundancy (in the sensor measurements) in the information received by the controller. In van Wyk et al (2019) they describe sensor anomaly detection in automated vehicles dependent on real-time exchange of information between vehicles and roadside infrastructure. Anomalous sensor readings caused by cyber-attacks or faulty vehicle sensors can result in crashes. They develop an anomaly detection approach through combining a deep learning method, with anomaly detection, that can detect anomalies and identify their sources.

Resilience in control systems: In Naufal et al (2018), safety is highlighted as a key foundation of autonomous vehicles. The work is based on a framework, supported by a normative risk process and an autonomous supervision and control system that aims to minimize the probability of vehicle collision hazard by employing resilient actions at run-time, reducing risks in the automotive transportation domain. Further they pointed out the need for a test-bed to evaluate safety and resilience for automotive cyber-physical critical systems. Biron et al (2017) describe mitigation of Denial of Service (DoS) attacks through a resilient control scheme for a platoon of connected vehicles equipped with Cooperative Adaptive Cruise Control. In Gutierrez et al (2019), the authors describe an intrusion detection system that could increase resilience and safety of advanced driver-assistance systems (Adaptive Cruise Control; Lane Centring Systems) and other autonomous systems. The vehicles are vulnerable since they are Internet-enabled devices with navigation, and entertainment. It is possible for an attacker to get access through these systems and gain control of the vehicle, but the intrusion detection system will improve safety and resilience. Halba et al (2018) establish resilient in-car communication solutions through reconfigurable networking. In Jeon et al (2019) they described an estimation system in an observer-based controller, that achieves resilience under cyber-attacks. Simulations showed that the estimation system was able to detect either a fault in the velocity measurement or a cyber-attack. In Li et al (2019) there is a description of trust-based control and scheduling for a platoon of unmanned ground vehicles (UGV) under cyber-attack. An algorithm, RoboTrust, is designed to analyse vehicle trustworthiness and eliminate information with low credit. A human operator scheduling algorithm is proposed when the number of abnormal UGVs exceeds the limit of what human operators can handle. The platoon survivability has been improved when compared to those that operate without this system. Liu et al (2019) provide a description of a resilient position estimate for autonomous vehicles under deception and DoS attacks. In Marquis et al (2018), they describe techniques to protect against sensor attacks on cyber-physical systems, using a resilient version of the Kalman filtering together with a watermarking approach to detect cyber-attacks and estimate the correct system state. Subke and Moshref (2019) focus on vulnerabilities and resilience of communication system in autonomous vehicles vs cyber-attacks.

Design of LoA transitions: In Flemisch et al (2019), they are discussing challenges related to safety critical transitions between different LoA. An example is the unsafe valley of automation between SAE LoA 2 (human in control) and level 4 (automation in control). There is a need for proper understanding and design of modes and transitions at the system limits (i.e. to build bridges) to improve the performance, safety and usability. They want to explore interaction and cooperation design based on a combination of the

driver's takeover ability and the controllability of the automation.

Testing schemes for resilience: D'Ambrosio et al (2019) point out that automated driving systems makes safety-critical decisions in complex environments. Resilient behaviour in their operation design domain is essential. They describe developments in Model-Based Systems Engineering (MBSE) to develop resilient safety-critical automated systems to provide guarantees about system behaviour. The methods focus on two aspects: ensuring resilient behaviour through Resilience Contracts for system decision making; and simulation-based testing to verify the system handles all known scenarios and validate the system against potential unknown scenarios. In Fowler et al (2018) they describe the fuzz test, a black box testing method used to find security weaknesses, in the vehicle's Controller Area Network bus and the vehicle's Electronic Control Units. The fuzz test has a part to play as one of the many security tests that a vehicle's systems need to undergo before being made ready for production. In Jha et al (2018) they describe methodologies for testing through fault injection for autonomous vehicles. In Park et al (2017); they identify a resilient linear classification scheme to deal with attacks and tampering on training data, used to train autonomous systems and vehicles. In Rubaiyat et al (2019) the used a Systems-Theoretic Process Analysis (STPA) based fault injection framework to assess the resilience of a driving agent, under different environmental conditions and faults affecting sensor data. The experimental results show that the proposed fault injection approach increases the hazard coverage compared to random fault injection and, help with more effective simulation of safety-critical faults and testing of autonomy.

3.3 *Air*

Aviation has implemented partial automation and have an impressive safety record, but we found few papers exploring successes. To summarise the papers, resilient architecture has been explored in unmanned aerial systems (UAS); resilience of control schemes has been suggested in manned flights and in UAS (to mitigate attacks); resilient physical design has been implemented to ensure improved reliability.

Resilient architecture: In Clifford et al (2017) they are trying to develop UAS swarms, as resilient autonomous systems to be able to navigate through hostile environments while performing intelligence, surveillance, and reconnaissance tasks, while minimizing the loss of assets. The research is developing a distributed multi-layer autonomous UAS, incorporating artificial life concepts, divided into three biologically inspired layers. These layers are the cyber-physical, the reactive, and the deliberative. Fast-reactive control systems in the cyber-physical and reactive layers ensure a stable environment supporting cognitive function at the deliberative layer. The team has developed the layered architecture and is observing success in developing reasonable behaviours in agents for prototype scenarios. In Madni et al (2017b), they suggest a resilient design approach based on Contract Based Design to create a Resilient Contract, to model complex systems with sufficient flexibility to incorporate resilience mechanisms. The target application domain is multi-UAS swarm control in uncertain, potentially hazardous, dynamic environments. Van Der Heijden et al (2018) describe cooperative adaptive cruise control - to bring more efficient and faster transportation through cooperative behaviour between vehicles (i.e. platooning), however this requires resilience against attacks. The results suggest a combination of misbehaviour detection and resilient control algorithms with graceful degradation are necessary for secure and safe platoons.

Resilience in control systems: In Sherry (2014), they discuss design for resilience in autonomous systems based on learning from controlled flight into stall accidents. Resilience can be achieved by the intervention of a human operator when the autonomous system creates an undesired state. The paper describes an analysis of the requirements and the design for this intervention in the operation of an autonomous function. In Marshall et al (2017a) and (2017b) autonomous system resilience during uncertainty is discussed. The authors propose a decision engine based on situational awareness and operational context, where the concept supports the optimization of satisficing behaviour. They focused on autonomous aircraft collision avoidance to increase autonomy in air traffic management, with improvements in mean success rate for the mitigation disruptions; mean time between violations committed during system operation and mean time to failure. In Marshall et al (2018) this is adapted to a context-driven decision engine for resilient command and control of air traffic management for autonomous aircraft operations. Results suggest that the context-based autonomy solution can enhance system resilience in comparison to the rule-based autonomy approach and enhance system resilience in comparison to the utility-based autonomy approach. In Yoon et al (2017); they describe concepts to develop attack resilient UAS. It is difficult to secure UAS platforms due to their openness and increasing complexity. They present a software architecture that enables an attack-resilient control of UAS. The framework provides mechanisms to monitor physical and

logical behaviours and to detect security and safety violations. They demonstrate how the framework can ensure the robustness of the UAS in the presence of security breaches.

Resilience in (physical) design: In Briod et al (2014), they utilize a physical enclosure design (gimbal) and described a collision-resilient and robust flying robot; that can fly efficiently in GPS-denied cluttered environments, being capable of colliding into obstacles without compromising their flight stability. Field experiments has demonstrated the robot's ability to fly fully autonomously through a forest while experiencing multiple collisions. Khedekar et al (2019) describe contact–based navigation path planning for aerial robots, called flying cartwheel that offers navigation resilience when the system is tasked to move in contact with surfaces that are otherwise non-traversable.

3.4 *Sea*

Resilience are increasingly being explored in autonomous shipping, and experiences from other modes are useful. To summarise the papers, strategies for resilience in design are described and the performance boundaries are highlighted as key strategies; resilience in communication are important; resilience engineering to improve safety should be prioritized since consequences may increase in unmanned shipping operations.

Resilience in Design: In Nuss et al (2016), they give an overview of unmanned maritime systems (UMS). As UMS are being deployed they will meet disruptions that affect their ability to satisfy their mission, thus resilience needs to be considered during the development. The paper discusses UMS, their high-level characteristics, discusses important resilience attributes and concludes with recommendations for further research. Insaurralde (2013) discusses strategies for resilience in control systems in autonomous marine vehicles. AMVs are required to carry out complex tasks and longer missions, that requires resilient operations and efficient resource management to succeed with minimal human interaction. Autonomic Computing (AC) capabilities are explored, such a self-healing, self-protecting, self-optimizing and self-configuring. Four strategies are discussed: AC capabilities as listed; Autonomic control paradigms; Autonomic software platforms and Robotic control architectures. In Gorman and Payne (2019), resilience is structured according to three distinct strategies: prevention, response, and recovery. Engineering for resilience in autonomous systems requires continuous active monitoring and control of system and subsystem performance. These control functions make an autonomous system cognitive in the sense that it works to identify and minimize influences that would disrupt its essential functioning. The system's resilience is its potential to continue to function in the face of irregular variations, disruptions, or degraded operating conditions. Dynamic systems analysis is discussed as a method to compute the risks, in pursuit of better reliability assessment of systems with autonomous control. In Mullins et al (2019) they explore testing methods for evaluating the resilience of Autonomous Unmanned Underwater Vehicles (UUV). The resilience of UUV can be defined as the vehicle's ability to reliably perform its mission across a range of changing and uncertain environments. Resilience is critical when operating UUVs where sensor uncertainty, environmental conditions, and stochastic decision-making all contribute to variations in performance. A challenge in quantifying the resilience of UUVs is the identification of the performance boundaries—critical locations in the testing space where a small change in the environment can cause a failure in an autonomous decision-making system. The article outlines a methodology for characterizing the performance boundaries of an autonomous decision-making system in the presence of stochastic effects and uncertain vehicle performance. In Thieme & Utne (2017), they describe a process for developing safety indicators for the operation of autonomous systems based on safety barriers and resilience engineering. The indicators reflect planning, safety in operation, in daily decision-making, and by identification of improvements. A case study of an UUV shows that the proposed process leads to a comprehensive set of safety indicators.

Resilience in communication: In Höyhtyä et al (2017), they explore data communication challenges of autonomous ships to ensure resilient operations in different environments such as ports, deep sea and Arctic regions. Multiple wireless systems are needed to ensure capacity, latency and secure communication. A hybrid concept that integrates satellite and terrestrial system is defined and described. A key part of the concept is a connectivity manager that ensures quality of service (QoS) for communications.

Safety Challenges: Wróbel et al (2017) explore the safety impact of unmanned vessels on maritime transportation, based on a whatif analysis of hundred maritime accident reports. The aim is to assess the risks (probabilities and consequences) if the ship had been unmanned. The analysis reveals that the occurrence of navigational accidents (e.g. collision, grounding) can be expected to decrease while consequences resulting from non-navigational accidents (e.g. fire, ship loss due to structural failure) can be expected to be larger for the unmanned ships. Successful examples from other modes with unmanned systems, i.e. automotive, airborne, metro, prove that autonomous vehicles can be

operated safely, provided that the system is properly designed, hazards are anticipated and the lessons from the past are learned. To achieve this, resilience engineering should be adopted when designing unmanned ships.

3.5 *Metro/ Rail*

Metro/Rail has implemented automation and have an impressive safety record, but we found few papers exploring successes. To summarise the papers, learning from successes should increase to improve resilience; and resilience trough remote operations seems to increase.

Resilience trough learning from successes: Arenius & Sträter (2014) performed an accident and event analysis of German railways focusing on resilience; and pointed out that to deal with human error probabilities, they must be evaluated in light of their impact on the positive aspects of safety (i.e. analysis of "what goes right").

Resilience in control: In Brandenburger et al. (2019), they argue in favour of keeping the layer of resilience associated with the train driver (from a control centre) that enables remote supervision, diagnosis and intervention of automated rolling stock. A study shows positive acceptance, usability and perceived benefit to system resilience; and lower than optimal workload ratings indicating capacity for additional tasks.

4. Conclusions and further research

Key issues driving resilience have been the need for more reliable autonomy; challenges in human-machine interface; the need for emerging machine learning and resilience to assure safety; and reliability when executing missions in complex environments. Key findings from our review, has been summarized at the start of each mode section. These conclusions are then carried forward in the following:

- Resilience from other modes are beneficial, and should be explored more across modes.
- Safety and reliability are dependent on performance boundaries, the operational envelope and how boundary issues are treated. Resilient behaviour in their domain has been found to be essential to ensure safety and reliability in complex environments where safety-critical decisions must be made. Design of the operation domain/envelope to enable resilience is a key issue.
- Resilience has been prioritized from 2017. Resilience and reliability of transportation system is dependent on systems and infrastructure support (ITS), communication resilience and resilience of control systems that can improve travel time and capacity.
- Vehicles and the ITS infrastructure must be able to handle not only natural disturbances but also new attacks of malicious nature. Resilience are important to improve security.
- Human intervention are a key issue in resilient and reliable automation and must be integrated in design of technology and organisation. Design must resolve how human intervention can mitigate failures of automation.

Autonomy and automation in manned aviation has supported an extremely high safety record in personnel transportation, but few papers were found discussing the effect of resilience on aviation. Autonomy in metro/railway systems have a long and successful safety and reliability track -record, but we found few papers exploring the background for the success of these.. Further research is needed.

Acknowledgement

The paper has been funded by the SAREPTA project, from the Norwegian Research Council.

References

Avizienis, Algirdas, et al. "Basic concepts and taxonomy of dependable and secure computing." IEEE transactions on dependable and secure computing 1.1 (2004): 11-33.

Cummings, M. (2014). Man versus machine or Man+Machine. IEEE Intelligent systems,

Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). Resilience engineering: Concepts and precepts. Ashgate Publishing, Ltd.

Hobbs, A., & Shively, R. J. (2014). Human Factor Challenges of Remotely Piloted Aircraft. In 31st EAAP Conference (pp. 5-14).

National Academies of Sciences. (2018). Resilience in Transportation Planning, Engineering, Management, Policy, and Administration. Washington, DC:

Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. Human factors, 39(2), 230-253.

Petritoli, E., Leccese, F., & Ciani, L. (2017). Reliability assessment of UAV systems. IEEE International Workshop on Metrology for AeroSpace (MetroAeroSpace) (pp. 266-270).

SAE (2016). SAE International standard "J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems." Revised: 2016-09-30

Vagia, M., Transeth, A. A., & Fjerdingen, S. A. (2016). A literature review on the levels of automation during the years. What are the different taxonomies that have been proposed?. Applied ergonomics, 53, 190-202.

Waraich, Q. R., Mazzuchi, T. A., Sarkani, S., & Rico, D. F. (2013). Minimizing human factors mishaps in unmanned aircraft systems. ergonomics in design, 21(1), 25-32

Appendix A – Overview of publications

Table A1 provides a chronological list of the publications included in the literature review.

Journal articles
Liu et al (2019) *Filter-Based Secure Dynamic Pose Estimation for Autonomous Vehicles*
van Wyk et al (2019) *Real-Time Sensor Anomaly Detection and Identification in Automated Vehicles*
Mullins et al (2019) *Search- Based Testing Methods for Evaluating the Resilience of Autonomous Unmanned Underwater Vehicles*
Henschke (2019) *Trust and resilient autonomous driving systems*
Ahmed et al (2019) *Evaluation of Transportation System Resilience in the Presence of Connected and Automated Vehicles*.
Ratasich et al (2019) *A Roadmap Toward the Resilient Internet of Things for Cyber-Physical Systems*
Gorman & Payne (2019) *Using Resilience to Inform Autonomous System Reliability Assessment: A Concept for Autonomous Ships*
D'Ambrosio et al (2019) *An MBSE Approach for Development of Resilient Automated Automotive Systems;*
Ängskog et al (2019) *Resilience to Intentional Electromagnetic Interference Is Required for Connected Autonomous Vehicles*
Ganin et al (2019) *Resilience in Intelligent Transportation Systems (ITS)*
Marshall et al (2018) *Context-Driven Autonomy for Enhanced System Resilience in Emergent Operating Environments;*
Naufal et al (2018) *A Vehicle-Centric Safety Conceptual Framework for Autonomous Transport Systems*
Vachtsevanos et al (2018) *Resilient Design and Operation of Cyber Physical Systems with Emphasis on Unmanned Autonomous Syst*
Thieme & Utne (2017) *Safety performance monitoring of autonomous marine systems*
Wróbel et al (2017) *Towards the assessment of potential impact of unmanned vessels on maritime transportation safety*
Nuss et al (2016) *Toward Resilient Unmanned Maritime Systems (UMS);*
Briod et al (2014) *A Collision-resilient Flying Robot*
Insaurralde (2013) *Autonomic computing technology for autonomous marine vehicles;*
Zieba et al (2011) *Using adjustable autonomy and human–machine cooperation to make a human–machine system resilient –*
Zieba et al (2010) *Principles of adjustable autonomy: a framework for resilient human–machine cooperation*
Conference papers
Flemisch et al (2019) *Human System Integration at System Limits and System Failure of Cooperatively Interacting Automobiles:*.
Gutierrez et al (2019) *Detecting Attacks against Safety-Critical ADAS based on In-Vehicle Network Message Patterns;*
Khedekar et al, (2019) *Contact–based Navigation Path Planning for Aerial Robots;*
Subke & Moshref (2019) *Improvement of the Resilience of a Cyber-Physical Remote Diagnostic Communication System*
Li et al (2019) *Trust-Based Control and Scheduling for UGV Platoon under Cyber Attacks*
Brandenburger & Naumann (2019); *Towards remote supervision and recovery of automated railway systems*
Rubaiyat et al (2019) *Experimental Resilience Assessment of An Open-Source Driving Agent;*
Bucic et al (2019) *Graph-Based Controller Synthesis for Safety-Constrained, Resilient Systems*
Jeon et al (2019) *Resilient control under cyber-attacks in connected ACC vehicles*
Fowler et al (2018) *Fuzz testing for automotive cyber-security*
Halba et al (2018) *Robust Safety for Autonomous Vehicles through Reconfigurable Networking;*
Jha et al (2018) *Fault Injection for Autonomous Vehicles*
Marquis et al (2018) *Toward Attack-Resilient State Estimation and Control of Autonomous Cyber-Physical Systems*
Van der Heijden et al (2018) *Analyzing Attacks on Cooperative Adaptive Cruise Control*
Wied et al (2018) *Resilient design properties of a driverless transport system*
Biron et al (2017) *Resilient Control Strategy under Denial of Service in Connected Vehicles*
Clifford et al (2017) *Multi-Layer Model of Swarm Intelligence for Resilient Autonomous Systems*
Höyhtyä et al (2017) *Connectivity for Autonomous Ships: Architecture, Use Cases, and Research Challenges*
Klingensmith & Madni (2017) *Resilience Concepts for Architecting an Autonomous Military Vehicle System-of-Systems*
Madni et al (2017a) *Model-Based Approach for Engineering Resilient System-of-Systems: Application into Autonomous Vehicle New.*
Madni et al (2017b) *Formal Methods in Resilient Systems Design: Application to Multi-UAV System-of-Systems Control*
Marshall et al (2017a) *Intelligent Control & Supervision for Autonomous System Resilience in Uncertain Word*
Marshall et al (2017b) *Adaptive and Automated Reasoning for Autonomous System Resilience in Uncertain Worlds*
Park et al (2017) *Resilient Linear Classification: An Approach to Deal with Attacks on Training Data;*
Ray (2017) *Transportation Security in the Era of Autonomous Vehicles: Challenges and Practice;*
Yoon et al (2017) *VirtualDrone: Virtual Sensing, Actuation, and Communication for Attack-Resilient Unmanned Aerial Systems*
Khan et al (2016) *Automation in driving for enhancing resiliency in transportation system*
Arenius & Sträter (2014) *Resilience engineering in railways—results from a systemic accident and event analysis in German railways*
Bezzo et al (2014) *Attack Resilient State Estimation for Autonomous Robotic Systems*
Sherry (2014) *Design for Resilience in Autonomous Systems: Lessons Learned from Controlled Flight into Stall Accidents*