Back to top

The Emergency Responsive Digital City[1]

Matthias Hollick*, Anne Hofmeister*, Jens Ivo Engels[a], Bernd Freisleben[c], Gerrit Hornung[b], Anja Klein[a], Michèle Knodt[a], Imke Lorenz[a], Max Mühlhäuser[a], Peter Pelz[a], Annette Rudolph-Cleff[a], Ralf Steinmetz[a], Florian Steinke[a], and Oskar von Stryk[a]

* contact authors: Department of Computer Science, SEEMOO, Technische Universität Darmstadt, Germany; (mhollick; ahofmeister)@seemoo.tu-darmstadt.de

[a] Technische Universität Darmstadt, Germany, [b] Universität Kassel, Germany, [c] Philipps-Universität Marburg, Germany

ABSTRACT

In 2050, roughly two-thirds of the world population are expected to live in urban areas. The sustainable growth in number and size of cities is only possible due to gains in efficiency in (critical) infrastructures such as energy, transportation, logistics, and water. Information and communication technology (ICT) is the main driver behind these efficiency gains and acts as the enabler for digital cities. The functioning of digital cities is at peril due to man-made or natural disasters, terror, and crises in general. Therefore, we argue that a paradigm shift towards resilient digital cities is imperative. Within the emergenCITY initiative, we aim to show that the resilience of digital cities can be enhanced through ICT, yet only if ICT itself is resilient. emergenCITY addresses the challenge to morph and utilize existing heterogeneous and amorphous ICT systems in all stages of the crisis. The goal for ICT in digital cities is to transition towards a self-configuring, self-healing, self-optimizing, and self-protecting way of operation, even if outside the original design envelope, while taking into account human interaction. emergenCITY facilitates a paradigm shift in how digital cities are conceived. It enables resilience through ICT by raising ICT resilience to the next level.

Keywords: Resilience, digital city, information and communication technology (ICT), cyber-physical systems

1 MOTIVATION

Urbanization is one of the most influential global trends. In 2050, roughly two-thirds of the world population are expected to live in urban areas; compared to only 30 percent in 1950 and 50 percent in 2010. The sustainable growth in number and size of cities is only possible due to gains in efficiency in (critical) infrastructures such as energy, transportation, logistics and water. Information and communication technology (ICT) is the main driver behind these efficiency gains. At the same time, we observe another urban trend: digitization. Internet, mobile broadband communication and the Internet of Things become increasingly important. Digitization affects and transforms society in a fundamental way. It is key to the reliable and efficient functioning of current and future cities.

However, both trends also pose a threat to the functioning of cities in crisis situations. Increasing interconnectedness and dependence on digital services make societies more vulnerable to disruptive events that impact on regular ICT functions. ICT-based infrastructures are at peril due to man-made or natural disasters, violence and terror. Most prominent are for example the events during the Tōhoku earthquake and tsunami in 2011. But also small crisis events can cause significant damage and disrupt the functioning of ICT infrastructure in cities. Worldwide the risks and the costs of natural disasters as well as the risk of localized cyber threats and terror attacks are rising.

In this context, the concept of resilience is of utmost importance. Resilience is the *ability of a system to cope with perturbations* such as crises and shocks while preserving its functions. Features of a resilient

[1] This conceptual paper presents the research focus of the interdisciplinary research initiative emergenCITY. The team is comprised of experts in the fields of computer science, electrical engineering, information technology, mechanical engineering, political science, history, architecture, and law.

system include at least one of the following*: absorption, recovering ('bouncing back'), adaptation and transformation ('bouncing forward')* [1]. Given the severe threats to the functioning of modern cities, designing and building resilient ICT with inbuilt emergency-responsiveness is one of the grand challenges for our society. However, it has only been investigated superficially. Traditional risk-based approaches to crisis management are not sufficient to deal with the increasing complexity of crises in today's complex and networked societies.

2 A New Paradigm for Resilience Research

To meet this challenge, we propose a novel paradigm: an ICT-centered, yet interdisciplinary, holistic approach to increase resilience of digital cities. According to our vision, future digital cities will possess the ability to adapt to all kinds of crises in an autonomous and self-organizing way, using heterogeneous, amorphous ICT systems. Future digital cities must be able to operate a basic ICT during times of crisis, in order to deal with the crisis and to move back to normal and efficient operation as smooth as possible. Our goal is to investigate fundamentals, methods and solutions towards enabling so-called „Resilient Digital Cities". With this, we refer to the resilience of future digital cities and the capability of ICT and its users to resist, adapt, and transform in crisis situations (see Figure 1).

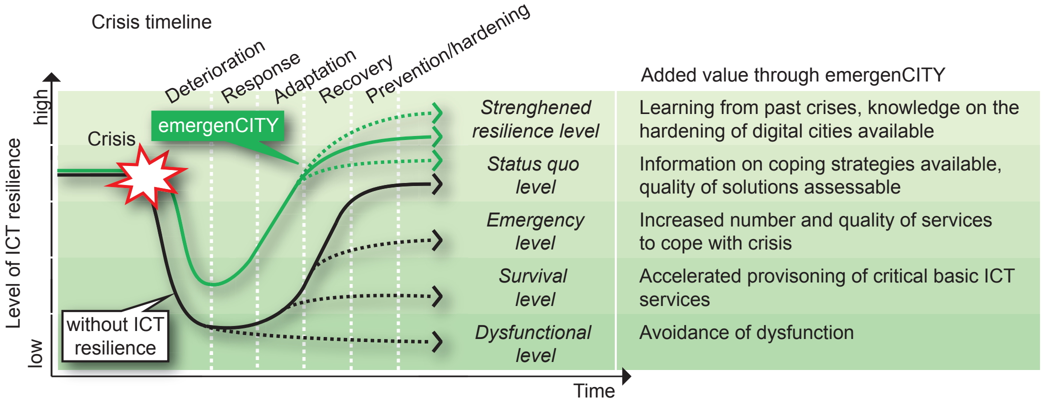


Figure 1: **Expected results of emergenCITY.** A crisis event disrupts the effectiveness of the digital city. emergenCITY aims to increase resilience of ICT in all stages of the crisis.

3 Scientific Approach

emergenCITY applies a multi-stage, interdisciplinary approach. Each stage of the crisis has specific frame conditions and requirements that have to be considered. Concepts for one stage must consider all other stages to produce innovative and efficient solutions (see Figure 2). We address the challenge to utilize existing heterogeneous and amorphous ICT systems—or sub systems that are still operational—in all stages of the crisis. The goal for ICT in digital cities is to transition towards a self-configuring, self-healing, self-optimizing, and self-protecting way of operation, even if outside the original design envelope, while systematically taking into account human interaction.

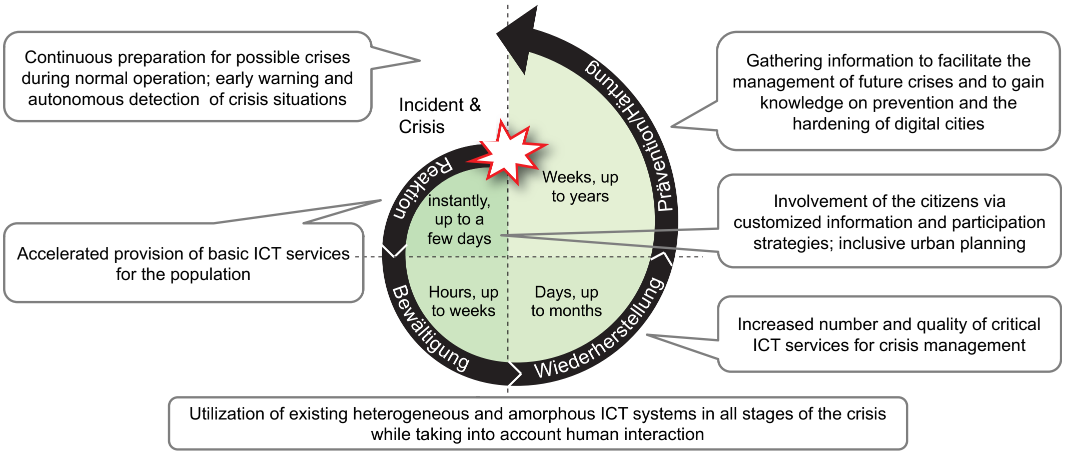

Continuous preparation for possible crises during normal operation; early warning and autonomous detection of crisis situations
Incident & Crisis
Gathering information to facilitate the management of future crises and to gain knowledge on prevention and the hardening of digital cities
Prävention/Härtung
Reaktion
instantly, up to a few days
Weeks, up to years
Involvement of the citizens via customized information and participation strategies; inclusive urban planning
Accelerated provision of basic ICT services for the population
Bewältigung
Hours, up to weeks
Days, up to months
Wiederherstellung
Increased number and quality of critical ICT services for crisis management
Utilization of existing heterogeneous and amorphous ICT systems in all stages of the crisis while taking into account human interaction

Figure 2: **Innovative research goals of emergenCITY during all stages of a crisis**

Back to top

3.1 Societal aspects/urban planning

We conceptualize the digital city as a socio-technical system. Therefore, our technological approaches and solutions are part of the political, social and cultural dimension of the city. We develop new governance concepts for the effective organization of ICT in crisis situations, involving public and private stakeholders in both horizontal and vertical coordination [2]. Governance and integrated urban planning are crucial to making cities inclusive, safe, resilient and sustainable (UN Sustainable Development Goal No. 11). A proactive and integrative approach to the design of public spaces is needed to ensure equal and fair access to basic services in the event of a crisis [3].

Legal aspects are covered particularly in the context of data privacy law. Different kinds of data, from social media posts to city-wide sensor grids can support de-escalation, emergency response, assessment of crisis situations and communication of public authorities and organizations with security functions. Collection and evaluation of this data must be in accordance with the law, but also future legislation may enable the increase of ICT resilience for crisis reaction. We further apply a historic perspective on large-scale disasters and analyze the “collective experience” of the population to (1) detect typical behavior patterns of the population and rescue teams and (2) reconstruct past learning processes of (non-digital) cities confronted with recurring catastrophes. This allows us to optimize future crisis reactions and learning processes for the resilient networked city [4].

3.2 Communication

In the area of *Communication*, we focus on the design of communication systems that have inbuild resilience and are responsive to any kind of crisis. These systems shall be able to self-prepare decentralized and infrastructureless operation prior to the disaster and to support basic communication services. In particular, we will focus on the concept of infectious networking for dynamic emergency network formation. We aim to analyze, design and build robust emergency networks under minimal assumptions from whatever communication devices currently available. During infrastructure failures, such networks could act as backup-networks to provide basic communication services [5].

In addition, we focus on heterogeneous probabilistic networking for situated networks. Following the development and deployment of robust and minimal emergency network configurations for situated networks, we analyze questions of service provision, dynamic reconfiguration, relevance assessment and prioritization [6]. We aim to optimize network configurations by applying new paradigms such as “probabilistic forwarding”. On device (in situ) processing and networking focuses on the role of hardware and firmware in emergency networks. We analyze the programmability of hardware and firmware and develop reactive, proactive, partial and dynamic reconfigurations of the system to instantiate new system functionalities that were not part of the original system design (“functionality morphing”).

3.3 Information

In the area of *Information*, we focus on autonomous composition of ICT services from whatever resources still available. A focus lies on mobile edge computing as well as distributed and decentralized services to support disaster response and recovery. In particular, we focus on resilience-centered multimodal data analysis on multiple time scales. We address the processing of information, which is initially not compatible for computer analysis (written and spoken language, visual information etc.), and focus on two aspects: (1) cross-modality, i.e. integrated processing of different forms of information and sources, and (2) cross-timescale integration, i.e. from emergency response in real-time to long-term data (data at rest) that can support preparation for future crises. Existing programming concepts and tools for developing and implementing resilient ICT systems vary substantially for different timescales: reactive or event-driven concepts dominate in the real-time domain, while classical-imperative (process-oriented) as well as functional and declarative approaches are applied in the long-term range ("data at rest"). We will create a new basis for software systems that integrate real-time and long-term data, including big data concepts such as probabilistic programming. A data-centric middleware for programming digital cities will be designed. The resilience of the resulting heterogeneous ICT-system will be evaluated by means of simulations.

Interaction concepts for data driven resilience planning complement these research topics. Information about cities is often complex and abstract. "Understanding" the data requires not only the adequate analysis and processing by the computer, but also the efficient and user-friendly interaction of humans with this data, especially when critical decisions are based on evaluations of crisis situations. In addition to the display and manipulation of information on a screen (city map) we develop ways to display information in the city itself, via Virtual and Augmented Reality as well as interacting 3D models [7].

Back to top

3.4 Cyber-physical systems

In the area of *Cyber-physical systems*, we focus on decentralized self-organization of critical physical infrastructures (energy, water, mobility/logistics) and local situation awareness and analysis. We apply a holistic approach to improve resilience of the critical infrastructures water and energy by ensuring self-organizing decentralized emergency operations. In the case of destroyed infrastructures, self-organizing decentralized systems that merge public and private infrastructure components, can contribute to context-driven protection and reestablishment of basic water and energy supply in crisis situations [8], [9]. In addition, we analyze how the resilience of mobility and logistics services can be increased through decentral self-organized ways of cooperation in cases of a degradation or loss of central information and traffic management systems. In this context, coordination of heterogenous cyber-physical agents is of utmost importance [10].

Semi-autonomous mobile robotic systems not only allow for emergency response and recovery in very complex environments. They further facilitate to (re-)establish communication backbones, i.e. through transport of mesh nodes. Local situation detection, awareness and analysis of a crisis situation is a key prerequisite for any measure to be taken by the different stakeholders. Therefore, autonomous ground and aerial robots are investigated for autonomous acquisition and real-time updates of the situation overview of a local crisis situation [11]. Different heterogeneous sensing modalities must be integrated including multi-modal scene analysis and novel through-wall and synthetic aperture radars for investigation of otherwise non-accessible interiors of buildings.

4 Conclusion

Overall, we must not only get a better understanding of the functioning of digital cities in cases of extreme events, crises, and catastrophes, but also develop fundamentals, methods, and solutions to enable so-called "Resilient Digital Cities". Our initiative emergenCITY works towards this end by applying a multi-stage, interdisciplinary approach to increase resilience in urban contexts. Therein, we aim to enable resilience through ICT by raising ICT resilience to the next level.

5 References

[1] D. Chandler and J. Coaffee, Eds., *Routledge Handbook of International Resilience*, Abingdon, United Kingdom; New York, NY, USA: Routledge, 2017.

[2] C. Fraune and M. Knodt, "Challenges of Citizen Participation in Infrastructure Policy-Making in Multi-Level Systems – The Case of Onshore Wind Energy Expansion in Germany," *European Policy Analysis*, vol. 3, no. 2, 2017, pp. 256-273, doi: 10.1002/epa2.1022.

[3] A. Rudolph-Cleff, "Transformative Capacities," in *Resilient Cities: re-thinking urban transformation*, N.Tollin, Ed., Book 3 - Planning Urban Resilience: Strategies, Frameworks and Integrated Planning Approaches for the Urban Resilience, forthcoming, pp. 1-13.

[4] J.I. Engels, Dangerous Water in the Land of the Economic Miracle. Hamburg's Flood Disaster in February 1962," in *Catastrophes. Views from Natural and Human Sciences*, A. Hoppe (Ed.), Heidelberg, Germany, 2016, pp. 123-134.

[5] F. Álvarez, L. Almon, P. Lieser, T. Meuser, Y. Dilla, B. Richerzhagen, M. Hollick, and R. Steinmetz, "Conducting a Large-scale Field Test of a Smartphone-based Communication Network for Emergency Response", in *Proc. of ACM CHANTS*, 2018, pp. 3-10, doi: 10.1145/3264844.3264845.

[6] S. Mueller, O. Atan, M. van der Schaar, and A. Klein, "Context-Aware Proactive Content Caching with Service Differentiation in Wireless Networks," in *IEEE Trans. WC*., vol. 16, no. 2, Feb. 2017, pp. 1024-1036, doi: 10.1109/TWC.2016.2636139.

[7] L. Wang, L. Jiao, T. He, J. Li, and M. Mühlhäuser, "Service entity placement for social virtual reality applications in edge computing," in *Proc. IEEE INFOCOM*, 2018.

[8] L. Rausch, J. Friesen, L. Altherr, M. Meck, and P. F. Pelz, "A Holistic Concept to Design Optimal Water Supply Infrastructures for Informal Settlements Using Remote Sensing Data," *Remote Sensing*, 2018, doi: http://dx.doi.org/10.3390/rs10020216.

[9] E. Kellerer and F. Steinke, "Scalable Economic Dispatch for Smart Distribution Networks", in *IEEE Trans. Power Systems,* vol. 30, no. 4, July 2015, pp. 1739-1746, doi: 10.1109/TPWRS.2014.235837.

[10] S. Kohlbrecher, J. Meyer, T. Graber, K. Petersen, O. von Stryk, and U. Klingauf, "Hector Open Source Modules for Autonomous Mapping and Navigation with Rescue Robots," in *17th RoboCup International Symposium*, 2014.

[11] L. Baumgärtner, S. Kohlbrecher, J. Euler, T. Ritter, M. Schmittner, C. Meurisch, M. Mühlhäuser, M. Hollick, O. von Stryk, and B. Freisleben, "Emergency communication in challenged environments via unmanned ground and aerial vehicles," in *Proc. IEEE GHTC*, 2017.

System Safety Assurance for Autonomous Vehicles (AV)

Lim Swee Nguan Henry, ST Engineering Land Systems Ltd, Singapore

Chong Xin Qian Sandy, ST Engineering Land Systems Ltd, Singapore

Keyword: System Safety, Autonomous Vehicles

Abstract

ST Engineering Land Systems (Land Systems) embraces Singapore's vision of a smart nation. As part of our drive towards smart urban mobility, we developed several Autonomous Vehicles (AV) for commercial and military applications. Owing to its complexity and stringent safety requirements, detailed analyses and extensive tests are needed.

With the increasing use of AV in today's world, system safety plays an important role to ensure its safe operation. The paper presents the system safety approach, hazard identification and the mitigation for the identified hazards and risks.

System Safety

Land Systems has been designing and producing armament and vehicle systems for its defence customers. These high risk systems can potentially cause catastrophic mishaps and hence applying system safety methods in all our products is of paramount importance. System safety approach is adhered throughout the system lifecycles; from concept till disposal. Over the years, MIL-STD-882 [1] has been used to define the system safety approach for safety assurance of our products.

System Safety Approach

Our system safety approach is well established for our defense products. Land Systems deploys this similar approach for the safety assurance of its AV projects. The approach can summarised as below.

1. Define scope of safety assessment and document the system safety approach
2. Identify hazards
3. Assess mishap risk
4. Identify mishap risk mitigation measures
5. Reduce mishap risk to an acceptable level
6. Verify mishap risk reduction
7. Review hazards and accept residual mishap risk by the appropriate authority
8. Track hazards, their closures and residual mishap risk

Software safety is an integral part of system safety and requires the necessary efforts to meet its identified Level of Rigor (LoR) [2]. Software Functional Hazard Analysis (FHA) is performed on the software functions to identify the software related hazards. Software criticality is also analysed based on the identified hazard severity and the software control category of the related software function [3].

Based on the analysed software criticality level, the required software LoR will be performed.

Scope of Safety Assessment

The scope of safety assessment defines the following:

1. Systems / Sub-Systems
2. Operational Environmental Factors

Back to top

The safety assessment scope covers the AV platform and the operational environment in which external entities such as trees, animals, other road users and the traffic control systems interact with the AV.

Identification of Hazards

The system safety practitioner has to understand the system architecture and functionalities of the AV well in order to identify the hazards related to malfunction of the systems in the AV. The FHA is a method used by the system safety practitioner in this case. By performing failure mode and irregularities analysis on all the system functions to identify the system related hazards.

The following Table 1 shows an example of the FHA on an AV project.

Table 1 – FHA Example

Function Record No.	Function Description	Failure Conditions	Operational Effects	Severity Category	Hazard Description
SRS-VCM-21	In Auto mode, on receipt of speed and curvature control commands, the VCM CSCI shall change to a computed steering wheel angle based on the curvature command	• Computes wrong steer command • Fails to output steer command	Vehicle unable to steer as intended May lead to possible vehicle collision	I	Loss of steering control function

Another method of identifying hazards is by brainstorming. Identify all possible top level mishap events such as vehicle collision and fire outbreak; and then analyse all possible hazards that could lead to the occurrence of such top level mishap events. Table 2 shows an example of the vehicle collision top level mishap event and some system hazards related to it.

Table 2 – Top Level Mishap & Related Hazards

Top Level Mishap	Event	Outcome	Hazards
Vehicle Collision	Vehicle unable to stop on time	Personnel death/ injury	Loss of brake control function
	Vehicle unable to steer as intended	Personnel death/ injury	Loss of steering control function
	Vehicle travels faster than intended	Personnel death/ injury	Loss of speed control function

For the operational related hazards, brainstorming is used to analyse the route(s) undertaken by the AV and analyse all possible hazards that could occur during navigation of these route(s). For example, programme manager, designers, testing team together with system and software safety practitioner will plan together a detailed route analysis and identify the potential hazards, risks and limitations of the AV performance under each specific route. Table 3 listed of some route navigations operational hazards.

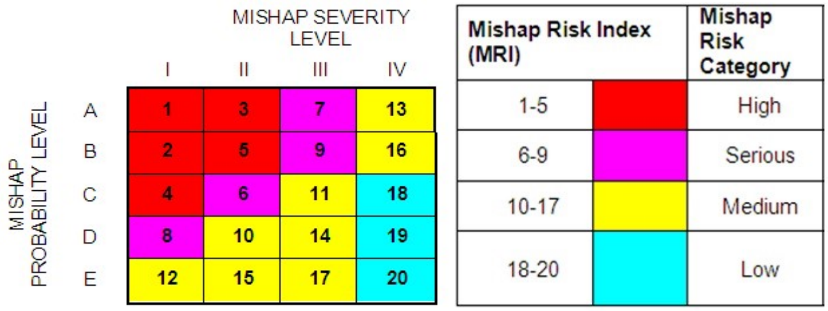
Table 3 – Operational Hazards

Top Level Mishap	Event	Outcome	Hazards
Vehicle Collision	Vehicle mounts kerb or collide with adjacent vehicles	Personnel death/ injury	Vehicle deviates from lane of travel
	Vehicle hits pedestrians at zebra crossings		Vehicle fails to give was to pedestrians at zebra crossing
	Vehicle hits other vehicle/ pedestrians at road junctions		Vehicle fails to cross traffic junctions safely
	Vehicle hits other vehicles at round about		Vehicle fails to give way to incoming vehicles at round about

Hazards can also be identified via similar project reference. Hazard analysis documentation from other similar AV related projects will be taken into consideration.

Mishap Risk Assessment

Mishap risk assessment seeks to assess the severity and probability of the identified hazards. Based on the hazard severity and probability from MIL-STD-882D, the mishap risk index (MRI) is derived. The system safety practitioner needs to ensure the residual risks of the identified hazards fall under the mishap risk category of “Medium” and “Low”. Refer to Figure 1 below.



MISHAP SEVERITY LEVEL

MISHAP PROBABILITY LEVEL	I	II	III	IV
A	1	3	7	13
B	2	5	9	16
C	4	6	11	18
D	8	10	14	19
E	12	15	17	20

Mishap Risk Index (MRI)		Mishap Risk Category
1-5	🟥	High
6-9	🟪	Serious
10-17	🟨	Medium
18-20	🟦	Low

Figure 1 — Mishap Risk Index

Hazard Mitigation

The system safety practitioner has to work closely with the project development team to lower the MRI of the identified hazards to as low as reasonably. Based on the MIL-STD-882D, the system safety order of precedence is used to introduce and implement hazard mitigations into the systems and operational processes. The hazard mitigations consist of safety design, safety devices, warning devices and lastly safety training procedures. These four areas form the system safety order of precedence.

Testing is an essential part of hazard mitigation for verification and validation. As AV technology and systems are evolving, the AV needs to be tested progressively and extensively before conducting live trials on the identified route(s).

Hazard Tracking & Closure

The hazard analysis needs to be documented for tracking and closure. An example of the hazard analysis documentation is shown in Figure 2.

Hazard Description	Causal Factor	Initial Risk	Mitigation	Residual Risk
Loss of brake control function	Malfunction of Drive by Wire (DBW) system due to: Hardware a) Internal system fault b) Loss of power supply Software c) Software failure to activate brake	ID	a) Designed Selection - Redundancy design (3x CPU, 2x Motors) - Backup batteries b) Safety Devices E-stop button to stop vehicle c) Warning Devices DBW failure alert d) Procedures & Training Safety operator to activate E-stop in event of emergency	IE

Figure 2 — Hazard Analysis Documentation

Upon mitigation of all identified hazards, the system safety working group will review the hazard analysis documentation. The system safety working group consists of the Chairman, panel members, system safety engineer(s) and the project development team. During the review session, they will review the following points:

1) Are all possible hazards identified?
2) Are the design mitigations adequate?
3) Are all design mitigations implemented and functioning correctly?
4) Are all operational safety procedures clearly defined and briefed?

When the system safety working group has reviewed the above points and endorsed the hazard analysis, only then the system(s) is assured safe for operational use.

Conclusion

Currently there is no universal global acceptance of a single safety standard associated with AV system. The recent TR 68 Technical Reference highlights that hazard analysis has to be done to ensure safe trial operation, which adopt a similar methodology as MIL-STD-882. Land Systems adopts the MIL-STD-882 methodology to ensure the safe operations of the AV system.

System safety assessment will be carried out at all levels addressing the concerns arising from various systems and sub-systems interacting within the operational environment. As the AV requirements and technologies are still evolving, more safety design and mitigation will need to be implemented. This will reduce the mishap risk level of the identified hazards to as low as reasonably practicable to ensure the developed systems are safe for operational use.

References

1. MIL-STD-882D, Department of Defense Standard Practice System Safety. Department of Defense (US), 10 Feb 2000.
2. Department of Defense, Joint Software Systems Safety Engineering Handbook, Version 1.0, 27 Aug 2010.
3. MIL-STD-882C, Military Standard System Safety Program Requirements, 19 Jan 1993.
4. TR 68, Singapore Standards Council Technical Reference Autonomous Vehicles, 8 Jan 2019.

Biography

Mr Lim Swee Nguan, Henry joined ST Engineering Land Systems as a System Safety Engineer in 2008. Since then he had been practicing system and software safety analysis for military projects such as the Next Generation Armoured Fighting Vehicle (NGAFV), the wireless Robotic Convoy and other autonomous system projects. He had previously assumed the role of System Safety Lead for the ongoing Autonomous Vehicle (AV) Bus project under Land Transport Authority (LTA).

Ms Chong Xin Qian, Sandy joined ST Engineering Land Systems as a System Safety Engineer in 2016. Since then she had been practicing system safety analysis for Autonomous Vehicle (AV) projects such as the Robotic Convoy and other autonomous bus projects the company is undertaking. She was also involved in the safety assurance of the 1st AV introduced to service at the Gardens by the Bay in 2018.