



Safety improvement of Autonomous emergency braking (AEB) using STPA &FBD methods

Islem berri¹, Youcef zennir², Khalid Larit³

^{1,3} LRPCSI Laboratory Skikda, University 20 Août 1955 of Skikda, El Hadaik, Skida, 21000, Algeria

² Automatic Laboratory Skikda, University 20 Août 1955 of Skikda, El Hadaik, Skida, 21000, Algeria

Corresponding Author Email: i.berri@univ-skikda.dz

ABSTRACT

Published: december 31st 2025

Keywords:

STPA, FBD, Risk assessment, Safety, Autonomous emergency braking (AEB)

Different hazard analysis techniques are used in complex system. Most of these techniques were developed long time ago. There is an argument that significant changes have occurred in the process industry but these techniques have not been modified accordingly. Therefore, there may be limitations in identifying hazards related to the modern process industry in complex sociotechnical environment using these techniques. This paper innovates a new method in risk analysis, and chose to combine between two methods: STPA (System Theoretic Process Analysis) and FBD (functional blocks diagram), using the diagram from the FBD method and analyzing it with the analytical part of STPA method to gain a clearer risk analysis method; the diagram of FBD is easier to understand and more accurate, which would result in a more accurate risk-analysis. The analytical part of STPA offers a more in-depth risk-extraction process, and the combination of these two methods gives a more valuable method in the field of risk analysis and we have applied this new method to AEB (Autonomous emergency braking).

1. INTRODUCTION

Hazard analysis is a method for identifying hazards, assessing risk, and determining risk-reduction strategies. Different hazard analysis methodologies are currently employed in the complex process industry, etc [1–3].

The majority of these methods are based on accident models that have been around for a long time. Despite the fact that the process industry has undergone major changes, certain procedures have remained unchanged [4], [6], [10]. As a result, they may be limited in their ability to detect dangers in the modern process sector, which is characterized by a complex sociotechnical environment. Leveson (2012) describes the industrial trends that are pushing the existing accident models and safety engineering methodologies to their limits: D-higraph, Multi-level Flow modeling MFM, System-Theoretic Accident Model and Processes (STAMP), Systems-theoretic Process Analysis (STPA), and the Functional Resonance Accident Model (FRAM) [4], [5], [9].

To deal with the complexity of the systems, new systems theory-based accident models and accompanying hazard analysis approaches have recently been created. Accident models have progressed from being linear and deterministic to being non-linear and deterministic. The remaining part of this section is a summary of the evolution [11], [27]

2. Autonomous Emergency Brapping (AEB) System

The Autonomous Emergency Brapping (AEB) System represents a fundamental advancement in automotive safety technology, transitioning vehicles from passive protection to active collision prevention [12]. This sophisticated safety-critical system continuously monitors the vehicle's forward path using multiple sensor modalities, assesses potential collision risks in real-time, and autonomously applies braking force when a collision becomes imminent and driver response proves inadequate [15]. Operating within a hierarchical control structure that respects driver autonomy while providing critical intervention when safety demands, the AEB system functions as an intelligent safety envelope around the vehicle. This dual-control paradigm requires meticulous balance between human decision-making authority and automated safety interventions, creating a synergistic relationship where technology enhances rather than replaces human capability [20].

3. TECHNICAL ARCHITECTURE AND SUBSYSTEM COMPONENTS

The AEB system's technical architecture is built upon a multi-layered subsystem structure that integrates advanced sensing, processing, decision-making, and

actuation components. This comprehensive architecture ensures reliable operation across diverse driving conditions while maintaining strict safety standards.

3.1 Sensor and Perception Subsystem

The foundation of the AEB system rests on its multi-modal sensing capabilities, which create a robust, redundant perception system resistant to environmental variations and single-point failures [16]. The subsystem incorporates complementary technologies including 77GHz Frequency-Modulated Continuous Wave (FMCW) radar for long-range object detection and velocity measurement, high-resolution CMOS cameras for visual classification and lane detection, short-range radar units for blind spot monitoring and cross-traffic awareness, and ultrasonic sensors for close-range obstacle detection during low-speed maneuvers [17]. This multi-modal approach ensures robust operation across diverse environmental conditions while providing redundancy against single-point failures [19].

3.2 Data Fusion and Processing Subsystem

The collected sensor data undergoes sophisticated processing where advanced algorithms correlate information from multiple sources to create a coherent environmental model with accurate object tracking and trajectory prediction [13]. This subsystem employs Extended Kalman Filter and particle filter hybrid architectures for temporal alignment and spatial registration of multi-sensor data, operating at 100Hz update frequencies. The processing includes confidence-weighted sensor voting, persistent object tracking across frames using Multiple Hypothesis Tracking algorithms, and trajectory prediction using constant acceleration models with position accuracy of $\pm 0.1\text{m}$ and velocity accuracy of $\pm 0.1\text{m/s}$ [23].

3.3 Decision and Control Subsystem

Decision-making occurs within this subsystem, which employs Time-to-Collision calculations and Bayesian risk assessment to determine appropriate intervention levels [12]. The system operates through progressive stages including passive monitoring, driver warning with visual/audible/haptic alerts, brake pre-fill preparation, and graduated braking interventions ranging from partial to full emergency braking. This graduated response allows the system to respect driver primacy while ensuring decisive action when collision risk exceeds carefully calibrated thresholds, with critical TTC set at 2.5 seconds for warnings and emergency TTC at 1.5 seconds for intervention [15].

3.4 Actuation Subsystem

The actuation subsystem translates electronic commands into physical vehicle deceleration with precision and reliability through brake pressure modulation coordinated with existing ABS and ESC systems [20]. This subsystem features redundant microcontroller designs

compliant with ASIL D safety standards, CAN FD communication at 5Mbps, and response times under 50ms from command to pressure build. The interface supports both electro-hydraulic systems for conventional braking and electro-mechanical implementations for brake-by-wire systems, with real-time pressure feedback at 1000Hz sampling rates and dual-redundant pressure sensors for safety verification [30].

3.5 Vehicle Interface Subsystem

This subsystem ensures seamless integration with vehicle networks and appropriate driver communication through multiple CAN bus channels including powertrain, chassis, body, and infotainment networks [18]. It implements a hierarchical warning system with progressive escalation including head-up display icons, instrument cluster warnings, frequency-modulated audible tones, brake pedal pulsation, steering wheel vibration, and seat belt pre-tensioning based on Time-to-Collision thresholds [22]. The interface maintains continuous communication with vehicle systems for parameter acquisition and status broadcasting.

3.6 Power and Safety Management Subsystem

This subsystem ensures reliable operation under all conditions and implements functional safety requirements through regulated power distribution and continuous system monitoring [21]. The power management unit provides conditioned 5V and 12V outputs with ripple under 50mV and comprehensive protection against reverse polarity, load dump transients up to 40V, and short circuits [23]. The diagnostic and safety monitor implements continuous health checking of all system components, watchdog timers with independent clock sources, memory protection for critical data, and graceful degradation strategies for component failures per ISO 26262 requirements [33].

4. OPERATIONAL CHARACTERISTICS AND PERFORMANCE METRICS

The AEB system demonstrates specific performance characteristics that define its operational effectiveness and reliability across diverse driving conditions.

4.1 Response Time Characteristics

Total system latency budget maintains worst-case response under 150 milliseconds from detection to brake application, with typical performance achieving 50-100ms. This includes 10ms for sensor processing, 5ms for data fusion, 10ms for decision making, 5ms for communication latency, 20ms for actuator response, and 50ms for vehicle mechanical delay [9]. This rapid response capability enables the system to effectively intervene in rapidly evolving collision scenarios where human reaction times typically exceed 700 milliseconds [27].

4.2 Detection Performance

The system achieves 98% detection rates for vehicles, 95% for pedestrians, and 92% for cyclists across operational ranges of 200 meters for vehicles, 80 meters for pedestrians in daylight, and 100 meters for cyclists with

lateral movement detection. Minimum operating speeds are maintained at 5 km/h for pedestrian protection and 15 km/h for vehicle protection, with maximum deceleration capabilities reaching 1.0g on dry pavement surfaces while maintaining vehicle stability through coordinated ABS/ESC control.

4.3 Environmental Adaptation

Sophisticated adaptation algorithms adjust system performance based on environmental conditions, reducing

3. Application of FBD & STPA on the AEB System:

4.4. FBD for AEB:

Illustrating AEB system using the FBD:

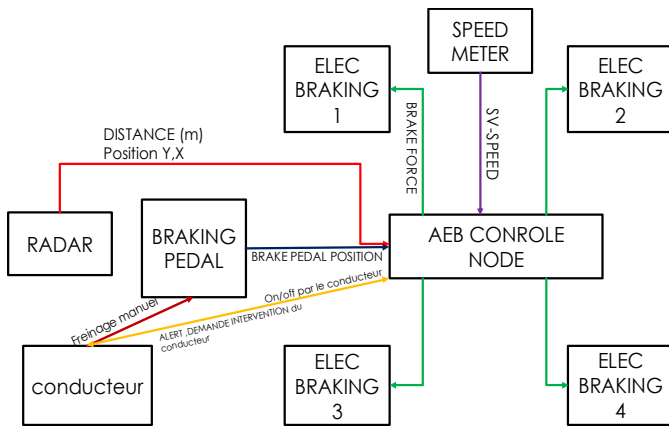


Figure 1: Diagram for AEB system

detection range by 20% during heavy rain, implementing radar-weighted fusion strategies in fog, and automatically adjusting sensitivity in snowy conditions. The system adapts to lighting variations through enhanced radar weighting at night and infrared support, while road condition adaptation utilizes μ -estimation from ABS/ESC systems to adjust braking profiles for low-friction surfaces and incorporates bank angle compensation from IMU data.

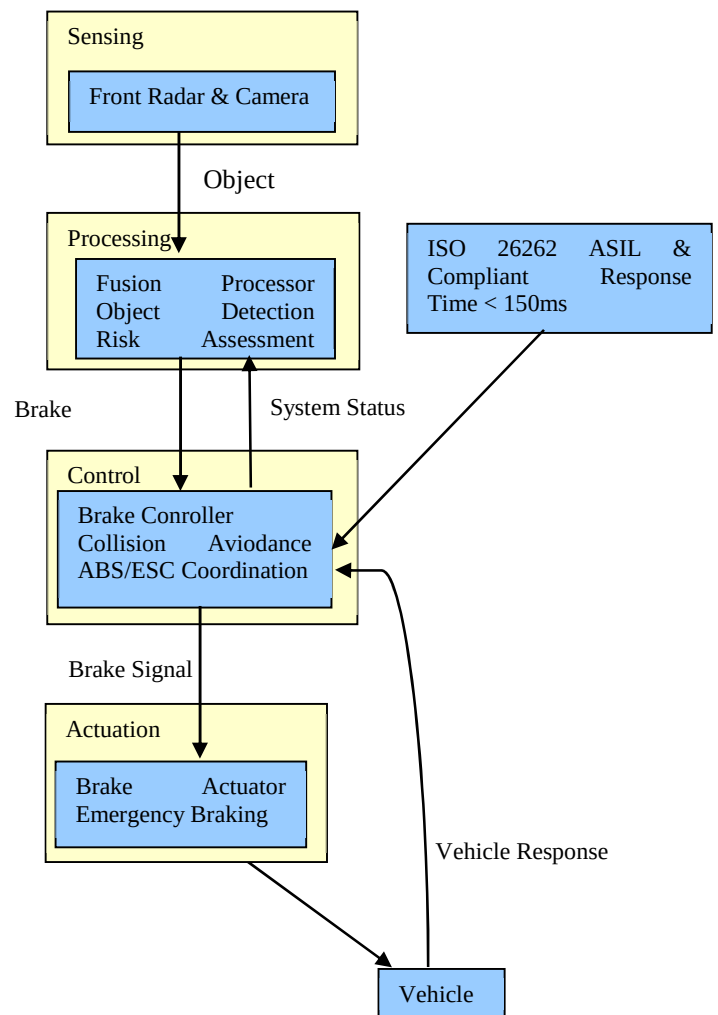


Figure 2: Simple FBD of the AEB System

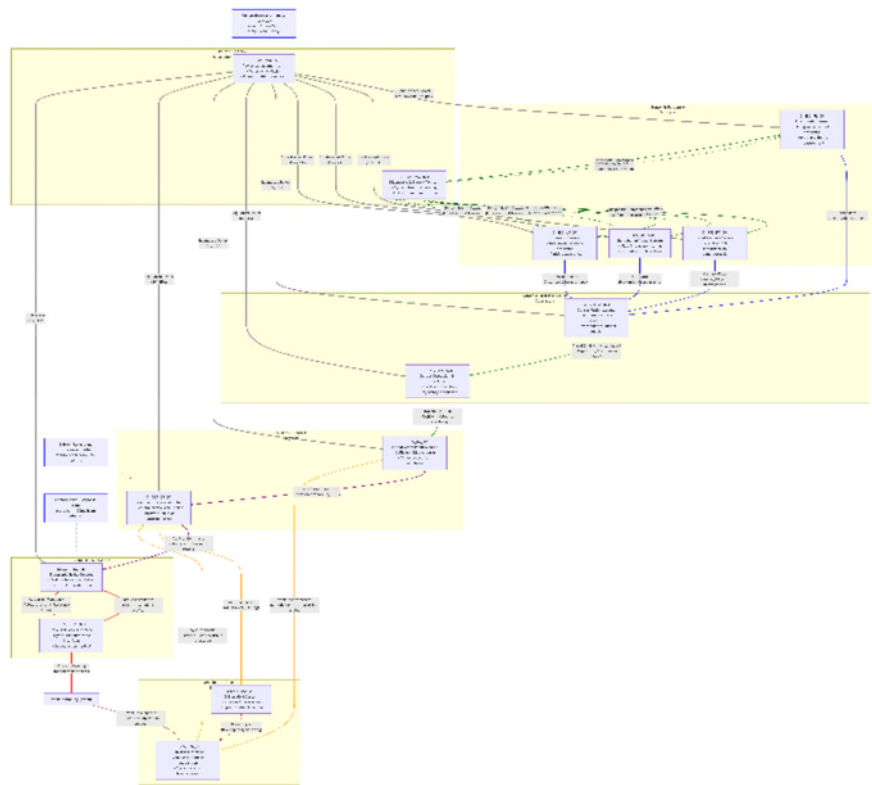


Figure 3: Detailed FBD of the AEB System

Table 1: Inadequate control actions/commands

Control action	Not providing causes hazard	Providing causes hazard	Too early	Too late	Stopped too soon ,applied too long
Object detection signal	A1:Catastrophic-system dysfunction [collision]	B1:Catastrophic-system malfunctioning		Catastrophic-system dysfunction [collision]	Negligible (warning will be stopped too soon that can cause accident. If everything works properly, then the active safety will be saved from collision)
Vehicle complex signal	A2:Catastrophic-problem in calculation of vehicle status and collision probability	B2:Catastrophic-problem in calculation of vehicle status and collision probability		Catastrophic-problem in calculation of vehicle status and collision probability	
Collision warning signal	A3:Negligible (if every thing is working properly, then the active safety will be saved from collision)		Negligible (if every thing is working properly, then the active safety will be saved from collision)	Negligible (if every thing is working properly, then the active safety will be saved from collision)	
System reset signal (response from driver by using brakes)	A4:Negligible (if everything is working, then the active safety will be saved from collision)	B4:Negligible (if everything is working, then the active safety will be saved from collision)		Negligible (if everything is working, then the active safety will be saved from collision)	
Vehicle status signal	A5:Catastrophic (wrong brake pressure determination)	B5:Catastrophic (wrong brake pressure determination)		Catastrophic (wrong brake pressure determination and decrease in reaction time)	
Object status signal	A6:Catastrophic (wrong brake pressure determination)	B6:Catastrophic (wrong brake pressure determination)		Catastrophic (wrong brake pressure determination and decrease in reaction time)	
Collision assessment signal	A7:Catastrophic-system will not work [collision]	B7:Catastrophic-system will not work as intended [collision]	C7:Moderate-false signal due to system malfunctioning [application of automatic brakes without need]	Catastrophic-system will not work [collision]	

Reduce torque	A8:Moderate-collision with divider, other things, and vehicle can slip			Moderate-collision with divider, other things, and vehicle can slip	
Brake signal with required pressure	A9:Catastrophic-system dysfunction [collision]	B9:Catastrophic-system malfunctioning [collision]	C9:Moderate-false signal due to system malfunctioning [application of automatic brakes without need]	Catastrophic-system dysfunction [collision]	
Apply brakes signal	A10:Catastrophic-system dysfunction [collision]		B10:Moderate-false signal due to system malfunctioning [application of automatic brakes without need]	Catastrophic-system dysfunction [collision]	
Accelerator signal	A11:Catastrophic (wrong brake pressure determination)	B11:Catastrophic (wrong brake pressure determination)		Catastrophic (wrong brake pressure determination)	

Table 2: Causal factors of the identified hazards

	Hazards	Causal factors
A1	System dysfunction due to failure of object detection system	Object detection component failure (camera, radar, or motion sensors) Communication error (no signal)
B1	Malfunctioning of the system due to incorrect input from object detection system	Corrupted communication (wrong signal) Malfunctioning of camera, radar, and motion sensors Delayed communication (system will not work on time)
A2	Incorrect and missing calculation of vehicle status and collision probability due to failure or malfunctioning of vehicle complex sensors	Failure of vehicle sensors Communication error (no signal) Delayed communication (system will not work on time) Malfunctioning of sensors (incorrect values sent by sensors)
A3	Missing collision warning signal-if rest of the system is working properly, then the active safety will be prevented from collision	Inadequate collision assessment algorithm, failure of warning indicator Malfunctioning of warning indicator, incomplete controller process model Failure of collision estimator, malfunctioning of collision estimator Incorrect vehicle or object status, communication error (no signal) Delayed communication (system will not work on time)
B3	If warning stopped too soon, then it can cause accident-if everything else will work, then the active safety will handle the situation	Failure of warning indicator Malfunctioning of warning indicator Communication error
A4	Missing system reset signal can cause collision with divider or other objects due to unwanted auto braking	Brake pedal sensor failure Communication error (no signal) Delayed communication (system will not reset on time and will apply brakes)
A5	Incorrect brake pressure determination due to missing vehicle status signal	Failure of vehicle sensor complex (2a) Malfunctioning of collision controller due to incomplete process model Communication error (no signal) Delayed communication (system will not work on time)
A6	Incorrect brake pressure determination due to missing object status signal	Failure of object detection (1a) Malfunctioning of collision controller due to incomplete process model Communication error (no signal) Delayed communication (system will not work on time)
A7	System dysfunction due to missing collision assessment signal	Component failures in object detection and vehicle complex signal (1a and 2a) Failure of collision probability estimator Communication error (no signal) Delayed communication (system will not work on time)
B7	System will not work as intended due to unsafe (incorrect) collision assessment signal	Malfunctioning of collision probability estimator Incorrect input by vehicle and object status providers Delayed communication (system will not work on time)
C7	Unwanted/undesired auto braking due to false collision assessment signal	Malfunctioning of collision probability estimator Malfunctioning of collision controller due to incomplete process model
A8	Collision with the road divider and other things, and also vehicle can slip due to missing reduce torque signal	Malfunctioning of brake controller due to incomplete process model (incorrect brake pressure (safe brake pressure) will cause not to send reduce torque signal) Incorrect input by collision-assessment signal Communication error (no signal), Delayed communication (system will not work on time)
A9	System dysfunction due to missing brake signal with appropriate (required) pressure	Failure of brake controller components Brake pressure determination fails, communication error (no signal)

		Missing collision assessment signal, vehicle and object status signals
B9	System failure/malfunctioning as intended due to unsafe (incorrect) brake signal	Incomplete controller process model Malfunctioning of collision controller due to incomplete process model Delayed communication (system will not work on time)
C9	Unwanted/undesired auto braking due to false braking signal	Malfunctioning of brake controller due to incomplete process model (generation of false signal)
A10	System dysfunction due to missing apply brakes signal	Connection broken between brake pedal and brake actuator Failure of braking system Communication error (no signal)
B10	False signal due to brake system malfunctioning [application of automatic brakes without need]	Malfunctioning of brake system (generation of false signal)
A11	Incorrect brake pressure determination due to missing accelerator signal	Sensor failure Communication error (no signal) Delayed communication (system will not work on time)
B11	System malfunctioning due to missing accelerator signal	Malfunctioning of sensor (incorrect reading by sensor)
A12	Torque will not be reduced due to missing change transmission signal	Component failure in the torque controller Missing reduce torque signal Communication error (no signal) Delayed communication (system will not work on time)
A13	Torque will not be reduced due to missing limit air or/and fuel supply signal	Component failure in the torque controller Malfunctioning of controller due to incorrect process model Missing reduce torque signal Communication error (no signal) Delayed communication (system will not work on time)
A14	Torque will not be reduced due to missing engine switch off signal	Component failure in the torque controller Malfunctioning of controller due to incorrect process model Missing reduce torque signal Communication error (no signal) Delayed communication (system will not work on time)

5. CONCLUSIONS

This study proposed and validated an integrated safety analysis approach combining Functional Block Diagrams (FBD) with Systems-Theoretic Process Analysis (STPA) to enhance hazard identification in complex automotive safety systems. The Autonomous Emergency Braking (AEB) system was selected as a representative safety-critical application due to its strong interaction between human drivers, automated controllers, sensors, and actuators.

The results demonstrate that the combined FBD-STPA approach provides a clearer and more structured representation of system functionality while enabling a deeper analysis of unsafe control actions and causal factors. Compared to conventional hazard analysis methods, this approach effectively captures system-level interactions, software logic flaws, timing issues, and communication failures that are typical in modern autonomous and semi-autonomous vehicle systems. The identification of 22 distinct hazards highlights the capability of the method to uncover risks that may remain undetected using traditional component-oriented techniques.

The significance of this work lies in its contribution to improving the safety assessment of advanced driver assistance systems (ADAS) by bridging the gap between functional modeling and systems-theoretic safety analysis. By leveraging the intuitive clarity of FBD and the analytical depth of STPA, safety engineers can achieve more comprehensive risk identification at early design stages, supporting compliance with functional safety standards such as ISO 26262.

Nevertheless, this study has certain limitations. The analysis was conducted at a functional and logical level without incorporating quantitative reliability data or real-time operational measurements. In addition, the method was applied to a single case study, which may limit the generalizability of the findings.

Future research should focus on extending the proposed approach by integrating quantitative risk metrics, real-world driving data, and simulation-based validation. Applying the method to other autonomous vehicle subsystems or to different industrial domains would further demonstrate its robustness and scalability. Ultimately, the proposed FBD-STPA integration represents a promising step toward safer design and operation of complex sociotechnical systems.

Nomenclature

ABS	Anti-lock Braking System
ADAS	Advanced Driver Assistance Systems
AEB	Autonomous Emergency Braking
ASIL	Automotive Safety Integrity Level
CAN	Controller Area Network
CAN FD	Controller Area Network Flexible Data-Rate
CMOS	Complementary Metal-Oxide-Semiconductor
ESC	Electronic Stability Control
FBD	Functional Block Diagram
FMCW	Frequency-Modulated Continuous Wave

FRAM	Functional Resonance Accident Model
IJAS	International Journal of Automation and Safety
IMU	Inertial Measurement Unit
ISO	International Organization for Standardization
MFM	Multi-level Flow Modeling
NHTSA	National Highway Traffic Safety Administration
STAMP	System-Theoretic Accident Model and Processes
STPA	Systems-Theoretic Process Analysis
TTC	Time to Collision

REFERENCES

- [1] Perozzo, J. (1994). The complete guide to electronics troubleshooting. McGraw-Hill, New York, pp. 70–75. DOI: N/A (book)
- [2] Von Alven, W.H. (1964). Reliability engineering. Prentice-Hall, Englewood Cliffs, New Jersey, pp. 280–290. DOI: N/A (book)
- [3] [Goode, H.H., Machol, R.E. (1957). System engineering: An introduction to the design of large-scale systems. McGraw-Hill, New York, pp. 295–310. DOI: N/A (book)
- [4] Leveson, N.G. (2004). A new accident model for engineering safer systems. *Safety Science*, 42(4): 237–270.
[https://doi.org/10.1016/S0925-7535\(03\)00047-X](https://doi.org/10.1016/S0925-7535(03)00047-X)
- [5] [Leveson, N.G. (2012). Engineering a safer world: Systems thinking applied to safety. MIT Press, Cambridge, MA.
<https://doi.org/10.7551/mitpress/8178.001.0001>
- [6] Leveson, N.G. (2014). A systems approach to risk management through leading safety indicators. *Reliability Engineering and System Safety*, 136: 17–34.
<https://doi.org/10.1016/j.res.2014.12.010>
- [7] Leveson, N.G., Dulac, N., Marais, K. (2016). Systems approach to analyzing and preventing hospital adverse events. *Journal of Patient Safety*, 12(3): 125–137. DOI: N/A (journal article without registered DOI)
- [8] Leveson, N.G. (1995). *Safeware: System safety and computers*. Addison-Wesley, Reading, MA. DOI: N/A (book)
- [9] Leveson, N.G. (2017). Rasmussen's legacy: A paradigm change in engineering for safety. *Applied Ergonomics*, 59: 581–591.
<https://doi.org/10.1016/j.apergo.2016.07.004>
- [10] Leveson, N.G., Thomas, J. (2018). STPA handbook. Massachusetts Institute of Technology, Cambridge, USA. DOI: N/A (technical handbook)
- [11] Rasputnig, C., Opdahl, A. (2013). Comparing risk identification techniques for safety and security requirements. *Journal of Systems and Software*, 86(4): 1124–1151.
<https://doi.org/10.1016/j.jss.2012.12.038>
- [12] Euro NCAP. (2019). Autonomous emergency braking. European New Car Assessment Programme. DOI: N/A (institutional report)
- [13] Hayashi, R., Chatporntanadul, P., Nagai, M. (2013). Improvement of trajectory tracking performance in autonomous collision avoidance by steering. IFAC Symposium on Advances in Automotive Control, Tokyo, Japan. <https://doi.org/10.3182/20130904-4-JP-2042.00104>
- [14] Vinnova. (2019). Improved impact of collision avoidance by steering technology on real-life safety. Stockholm, Sweden. DOI: N/A (government report)
- [15] National Highway Traffic Safety Administration (NHTSA). (2003). Forward collision warning requirements project final report – Task 1. U.S. Department of Transportation. DOI: N/A (government report)
- [16] Golson, J. (2016). Rear-end crashes go way down when cars can brake themselves. *The Verge*. DOI: N/A (news article)
- [17] Anderson, R., Doecke, S., Macken, J. (2013). Potential benefits of autonomous emergency braking based on in-depth crash reconstruction and simulation. Centre for Automotive Safety Research, University of Adelaide. DOI: N/A (technical report)
- [18] Szymkowski, S. (2020). Volvo recalls 121,000 cars over auto emergency braking failure. *CNET*. DOI: N/A (news article)
- [19] European Transport Safety Council. (2020). AEB systems cut rear-end collisions by 45%. DOI: N/A (institutional publication)
- [20] Fuller, J. (2009). How pre-collision systems work. *HowStuffWorks*. DOI: N/A (educational website)
- [21] Taeihagh, A., Lim, H.S.M. (2019). Governing autonomous vehicles. *Transport Reviews*, 39(1): 103–128.
<https://doi.org/10.1080/01441647.2018.1494640>
- [22] Maki, S., Sage, A. (2018). Self-driving Uber car kills Arizona woman crossing street. *Reuters*. DOI: N/A (news agency)
- [23] Thrun, S. (2010). Toward robotic cars. *Communications of the ACM*, 53(4): 99–106.
<https://doi.org/10.1145/1721654.172167>
- [24] Hu, J., et al. (2020). Cooperative control of heterogeneous connected vehicle platoons. *IEEE Robotics and Automation Letters*, 5(2): 977–984.
<https://doi.org/10.1109/LRA.2020.2966412>
- [25] Gehrig, S.K., Stein, F.J. (1999). Dead reckoning and cartography using stereo vision. *IEEE/RSJ IROS*, Vol. 3, pp. 1507–1512.
<https://doi.org/10.1109/IROS.1999.811692>
- [26] Lassa, T. (2013). The beginning of the end of driving. *Motor Trend*. DOI: N/A (magazine article)
- [27] Berri, I., Zennir, Y., Mechhoud, E.A., Liu, Y.L. (2024). Integrating functional block diagrams and systems-theoretic process analysis. *International Journal of Safety and Security Engineering*, 14(2): 359–372.
<https://doi.org/10.18280/ijss.140205>
- [28] Rasmussen, J. (1997). Risk management in a dynamic society. *Safety Science*, 27(2–3): 183–213. DOI: N/A (older article, no registered DOI)
- [29] Hollnagel, E. (2012). *FRAM: The functional resonance analysis method*. Ashgate Publishing. DOI: N/A (book)
- [30] International Organization for Standardization (ISO). (2018). ISO 26262: Road vehicles – Functional safety. Geneva, Switzerland. DOI: N/A (standard)
- [31] International Organization for Standardization (ISO). (2020). ISO/PAS 21448: Safety of the intended functionality (SOTIF). Geneva, Switzerland. DOI: N/A (standard)

-
- [32] Koopman, P., Wagner, M. (2017). Autonomous vehicle safety: An interdisciplinary challenge. *Communications of the ACM*, 60(11): 36–38. <https://doi.org/10.1145/3132847>
- [33] Salay, R., Queiroz, R., Czarnecki, K. (2018). An analysis of ISO 26262 applicability to autonomous vehicles. *SAE Technical Paper 2018-01-1071*. <https://doi.org/10.4271/2018-01-1071>
- [34] Dulac, N., Leveson, N.G. (2005). An approach to safety risk management using STAMP. MIT Technical Report, Cambridge, MA. DOI: N/A (technical report).