Sciences du Nord Nature Science and Technology
Vol. 2, No. 02, December 2025: pp. 182-194
E-ISSN: 3046-6504
P-ISSN: 3047-4922
DOI: https://doi.org/10.71238/snnst.v1i02.239

Launch-Gated Safety Architecture for Coordinated ADAS and Occupant Restraint Product Industrialization

Chethan Kanakuppe Siddegowda [1]
[1] Magna Electronics
Coresponding Author: Chethan.siddegowda@magna.com

ARTICLE HISTORY
Received Oct, 2025 **Revised Nov, 2025** **Accepted Dec, 2025**

ABSTRACT
Advanced driver assistance systems and occupant restraint systems now share signals, timing and safety objectives, but most suppliers still launch them separately. This loophole enables the interface flaws to work their way into production. A launch gated safety architecture having five release gates connecting the two product lines, shared readiness score, and deny overrides release rule have been proposed in this paper. The architecture integrates a functional safety, a safety of the purpose, a hazard analysis, a failure operational design, a virtual validation and a software update control. An approximate launch study then compares the proposed approach with an implicit base or utilizes the individual gates base. The research case involves twelve pre series constructions, 240 trial conditions and 84 seeded integration faults. The proposed method identified 77 defects prior to production and the baseline identified 57. The escape rate has dropped down to 8.3 percent from 32.1 percent. Last preparedness increased from 0.81 to 0.93. The criterion values of head injury in a pre-crash braking and a frontal crash case dropped by 21 percent when full tension was attained by the pretensioner with the right lead time. The reliability of a 0.95 component was improved by two out of three architectures to 0.993. There was a 2,000 to 20,000 factor reduction in the test distance required using importance sampling. Outcomes are explanatory and ready to learn.

Keywords: *ADAS; Fail Operational Architecture; Functional Safety; Launch Gate; Occupant Restraint; Pre Crash Braking; Product Industrialization.; SOTIF*

INTRODUCTION

Research on automated driving has been rapidly expanding, but safety is the primary obstacle to greater adoption. Through an extensive overview of automated driving systems, there are reports that the systems represent the safest and most efficient way of driving but accident-related fatalities are increasing and the strength of existing approaches must be strengthened [1].

The release problem is challenging as there is a large number of specialties that have a contribution to one vehicle function. Koopman and Wagner believe that the biggest difficulty lies in end-to-end design and deployment process bringing together safety concerns of most of the technical disciplines into one way [2]. That paper states the same that a failure uncommon to a single vehicle is in fact too common with a multitude of vehicles.

Occupant restraint is a second level of interaction. Emergency braking provided as part of an assistance feature alters the occupant position prior to the beginning of a crash. This was demonstrated in a human model full-frontal impact simulation that demonstrated that pre impact braking caused the occupant to move forward and increased both neck and thorax injury values,

and the authors indicated the importance of the integration between active and passive safety as a critical technical issue [3].

These two lines of products are usually made by suppliers in individual reviews. According to Riedmaier and co-authors, the market would not accept a launch without evidence of safety, neither in society nor by lawmakers, and they categorize scenario-based assessment as a promising path towards said evidence [4].

This paper makes three contributions. It establishes a five-gate launch gated safety architecture that shares a release rule. It connects every gate to design principles. It makes a report on a simulated launch study that transports the comparison of coordinated gating and separate gating.

LITERATURE REVIEW

2.1 Safety Standards and Architecture Foundations

The foundation process in electrical and electronic systems in road vehicles is specified in functional safety standards. A reference chapter on driver assistance states that ISO 26262 establishes standards to prevent or mitigate systematic failures as well as haphazard hardware failures [5]. Kölbl et al. note that the standard does not deal with autonomous driving functions per se, so they introduce a model-based approach that evaluates the functional safety of architectures along the traditional of standard and helps to evaluate their architectural variants [6]. A chapter on automated driving systems explores the extent to which the standard addresses complexity, availability, and state safety issues [7].

Machine learning brings yet another issue. According to Burton and others, the assurance case structure may be used to structure both the systems engineering and validation questions that are presented by learned functions in the highly automated driving scenario [8]. Confidence arguments of performance evidence are tested on a pedestrian recognition case later [9]. A gate should thus request evidences and not just completion of tests.

2.2 Hazard Analysis and Fail Operational Design

The methods of hazard analysis have to address the interrelations between functions. Hirata and Nadjm Tehrani use system theoretic process analysis and goal structuring notations to construct the safety argument [10]. Fail operational design is the focus as well. Sommer et al. explain the RACE architecture, which involves centralized topology, a run time environment with fail operational behavior, and spatial and temporal separation of resources [11]. Weiss and colleagues introduce the concept of SafeAdapt to turn the failure mode of operation of the electrical and electronic architecture into a general one at a reasonable cost [12].

Table 1 cross tabulates the reviewed themes with the contribution made by the themes to the gated architecture.

Table 1. Qualitative map of perceived research themes using the contribution made by each of the research themes and how it has been utilized by the launch gates.

Theme	Main contribution	Use in launch gates
Functional safety standards	Procedure on systematic and random failures	Defines evidence required at each gate

Machine learning assurance	Confidence arguments and assurance cases	Establishes standards of learned perception
Hazard analysis	Hazard identification that is influenced by interaction	Feeds the open hazard count in the release rule
Fail operational design	Safe degradation and redundancy	Establishes availability goals in advance of release
Occupant restraint interaction	Pre-crash effect on the occupant position	Declares the common timing interface
Virtual and loop testing	Testable sensors and controllers	Provides support to validation of design
Software update control	Guaranteed and accountable field changes	Prolongs the production life of the gates

2.3 Numerical Evidence from the Literature

Some of the reviewed articles provide figures that determine the study design. According to Zhao et al. importances sampling was used to prune the number of scenarios and the acceleration rates of approximately 2,000-20,000 to ensure that the 1000 simulated miles subject a vehicle to circumstances that require approximately 2-20 million real miles [13]. Van Marter et al. developed a deep learning in cabin radar system, and reported a classified accuracy of 95.6 percent localized occupant, and 88.7 percent organized an occupant as an adult, child, or baby [14]. The Koopman article above uses one billion operating hours per catastrophic event of a specific function as a target. These are tabulated in Table 2.

Table 2. Numerical data derived in the papers reviewed, including the value reported and why is important to the design of the gates to the launch gates.

Evidence item	**Reported value**	**Relevance to launch gates**
Scenario exposure acceleration	2,000 to 20,000	Establishes boundaries to virtual test planning
Miles (in the real world) divided by 1,000 simulated miles	2 to 20 million	Favors shortening of tests
Hours of operation per cat event	About 1 billion	Reasons why interface defects should close early
Accuracy of localized occupant detection	95.6 percent	Establishes a reference to the quality of a sensing input
Accuracy of adult, child, baby classification	88.7 percent	Shows limits of occupant state input
Minimization of radar calculation	54.1 percent	Demonstrates the data cost saving of sparse data
Cuts in radar data quantities	94.7 percent	Supports use of edge processing

2.4 Validation and Occupant Sensing

Virtual validation reduces the cost of test. Jasinski et al. describe a complete procedure to evaluate and optimize radar sensor models, as radar-based assistance systems can only rely on models of high fidelity prior to the belief in simulation results [15]. The camera in the loop system compares a real automotive camera with the simulated scenes and evaluates the specification by the manufacturer to test under conditions like bad weather that are difficult to duplicate on the road [16]. A hardware in the loop test injects sensor errors in the target control unit to evaluate target robustness in the lab [17].

PROPOSED LAUNCH GATED SAFETY ARCHITECTURE

3.1 Gate Structure and Readiness Score

The five gates are denoted in figure 1. Gate G1 considers the concept and the common safety objectives. Gate G2 solidifies design and specification of the interface. Design validation is confirmed by Gate G3. Process validation on the production line is done at the Gate G4. Gate G5 provides freedom to series production.

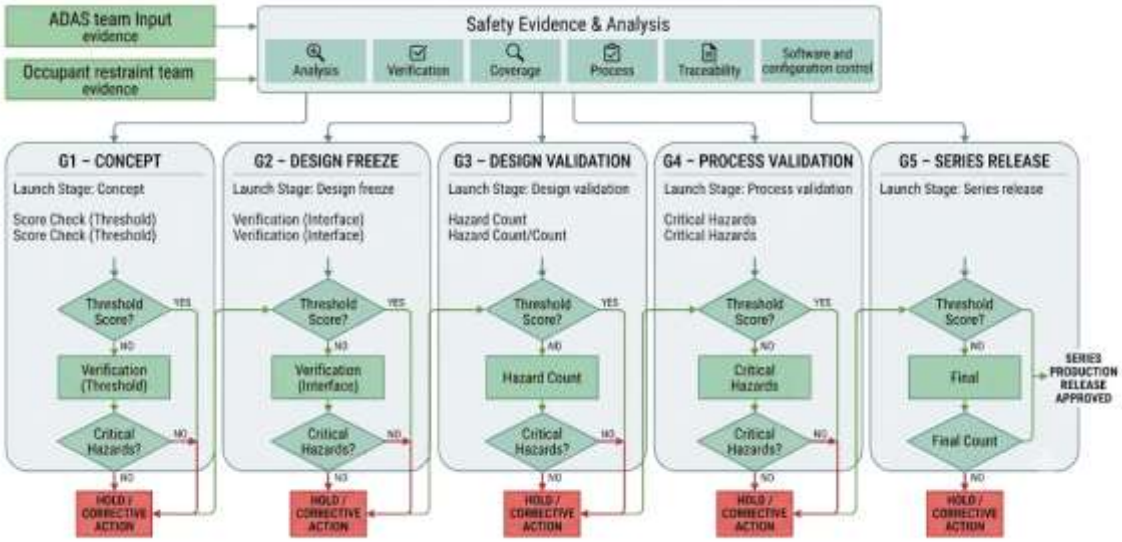


Figure 1. There are five launch gates G1-G5 with shared evidence provided by ADAS and restraint crews and a go on release or hold allocation at any launch gate

The gates compute a readiness score. In equation 1, the score is assumed to be a weighted average of five criteria scores from 0 to 1.

$$G_k = \sum_{i=1}^{5} (w_i \times s_i), \quad \text{with} \quad \sum_{i=1}^{5} w_i = 1 \tag{1}$$

The criteria are completeness of hazard analysis (weight 0.25), verification of interface (weight 0.25), test coverage (weight 0.20), process capability (weight 0.20), and traceability (weight 0.10). This evidence view is supported by a failure operational design approach where a judging of the suitability of an evolving architecture begins in the initial stages of the design, and a highway pilot study extends this to the realm of operational design [18].

Table 3 indicates the gate thresholds of the study.

Table 3. Gate limits comprising the readiness score, minimum interface verification score and the count of open critical hazards permitted at any given launch gate

Gate	Launch stage	Readiness threshold	Minimum interface score	Open critical hazards allowed
G1	Concept	0.60	0.50	4
G2	Design freeze	0.70	0.60	2
G3	Design validation	0.80	0.75	1
G4	Process validation	0.85	0.85	0
G5	Series release	0.90	0.90	0

The decision to release is subject to a deny overrides rule. Equation 2 makes the decision regarding the gate k that ensures the gate is released upon meeting the limits of the readiness score and the interface score and the number of open hazards.

$$\text{Release}_k = 1 \text{ if } (G_k \geq \tau_k) \text{ and } (I_k \geq \iota_k) \text{ and } (H_k \leq h_k), \text{ otherwise Release}_k = 0 \quad (2)$$

In this case, τ_k is the threshold of readiness, I_k is the score in interface verification, ι_k represents the minimum in interface verification, H_k is the number of open critical hazards, and h_k is the permitted number. Failure in one of the failed conditions implies non-release, despite passing the other two.

3.2 Coordinated Functional Architecture

The coordinated architecture is shown in figure 2. ADAS controller transmits time, collision, braking level, and confidence to a safety supervisor. The restraint controller is sent a pre crash command by the supervisor and it activates the reversible pretensioner and adjusts the level of load limiter. The restraint controller provides its health state and the occupant state. The supervisor is guided by the principle fail operational, according to which one defect impairs the functioning without safeguarding. This option is facilitated by concepts of fail aware, fail safe, and fail operational automated vehicles with hardware and software redundancy, implemented using ISO 26262 and ISO PAS 21448 [19].

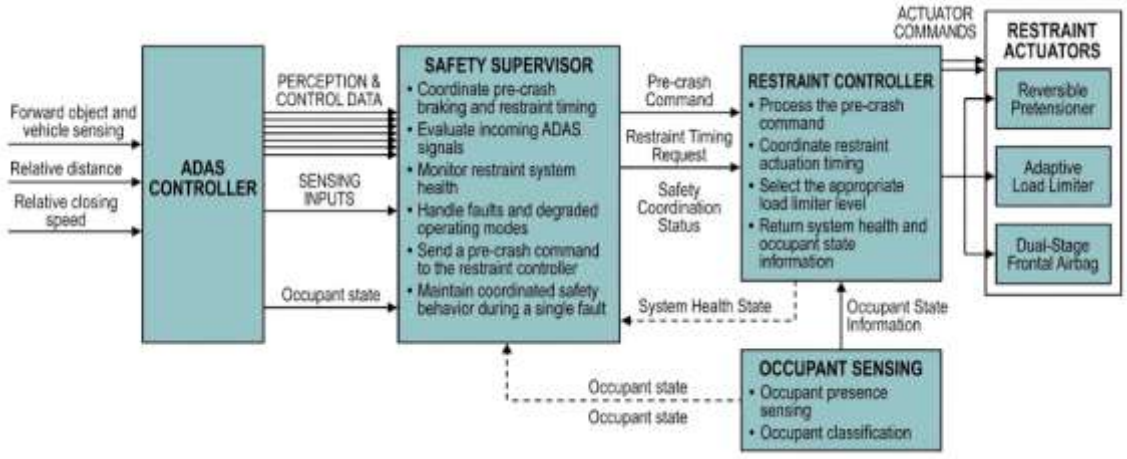


Figure 2. Integrated system connecting the ADAS controller, safety supervisor, restraint controller, occupant sensing and the pretensioner, load limiter and airbag actuators

Risks in this architecture are prioritized on the residual risk. The residual risk of hazard i is given by equation 3 and it is equal to exposure probability times severity times uncontrollability.

$$R_i = P_i \times S_i \times U_i \quad (3)$$

A combination of methods is employed in hazard identification. An overtaking assistant study uses hazard and operability study with step number 1 based on system theoretic process analysis method at vehicle level and failure mode and effects analysis with step number 2 used in the safety analysis [20]. The proposed architecture adopts the same combination for the shared interface. An assurance case about a learned chassis control functional indicates the way in which variations to previous ISO 26262 techniques are dealt with and in which the explainability and resilience to small changes in inputs justify the argument [21]. The deep networks have a verification framework to ensure that a classification remains the same within a small area of an input [22].

STUDY DESIGN

4.1 Launch Program and Test Set

The experiment is based on a simulated launch program of a combined forward braking system and a restraint system of a reversible pretensioner, an adaptive load limiter and dual stage frontal airbag. The data in Section 5 are simulated for demonstration. There was a comparison of two arms. An independent ADAS review and restraint review were conducted on the baseline arm. The five gates mentioned above were used in the coordinated arm. The twelve pre series builds and the set of 84 seeded integration defects were processed by both arms. Table 4 gives the configuration.

Table 4. Configuration of the simulated launch study that displays the amount of builds, test scenarios, seeded defects and sled tests, and the objective of each parameter.

Parameter	Value
Pre series builds	12
Gate reviews	5
Test scenarios	240
Braking trigger scenarios	120
Mixed pre-crash and crash scenarios	80
Fault injection scenarios	40
Seeded integration defects	84
Sled tests	36
Importance sampling factor	5,000

The seeded defects are 24 timing, 21 signal interface, 18 fault handling, 12 calibration and 9 process defects. Virtual tests worked with sensor models which were verified with the process in Section 2.4. The radar sensing performance in Section 2.3 was followed by the input of occupant

presence. This input option is aided by passenger surveillance based on the use of inexpensive millimetre wave radar and artificial intelligence [23].

4.2 Timing and Injury Metrics

The pretensioner requires maximum tension to be struck. The command delay is related to the time to collision in equation 4.

$$\mathrm{TTC} = \frac{d}{v_{\mathrm{rel}}}, \quad \text{and} \quad t_{\mathrm{cmd}} + t_{\mathrm{lead}} + t_{\mathrm{lat}} = \mathrm{TTC} \tag{4}$$

Here d is the distance to target, v_{rel} is the moving speed, t_{cmd} is the time between the braking trigger and the pretensioner command, t_{lead} is the lead time that is required to reach full tension before impact, t_{lat} is the latency of the actuator. When the gap between the two bodies is 20 m and the closing speed is 13.9 m/s, the time to their collision is 1.44 s. The command has a lead time of 0.20 s and a latency of 0.15 s, which means that the command should be issued 1.09 s following the trigger.

The head injury criterion is used to measure head injury in Equation 5.

$$\mathrm{HIC}_{15} = \max_{t_1,t_2}\left[\Delta t \times \left(\frac{1}{\Delta t}\int_{t_1}^{t_2} a(t)\, dt\right)^{2.5}\right], \quad \text{with } \Delta t = t_2 - t_1 \le 15 \text{ ms} \tag{5}$$

where a(t) head resultant acceleration in g. Three types of sled were used. Configuration A used braking only. Configuration B involved the use of a pretensioner having a lead time of 0.05 s. Configuration C used a pretensioner with the coordinated lead time of 0.20 s.

4.3 Reliability and Test Acceleration

Availability targets assume a two out of three-voting system. The reliability of such a structure is found in equation 6 as a function of the reliability R of a single channel.

$$R_{\mathrm{sys}} = 3R^2 - 2R^3 \tag{6}$$

The result is plotted in figure 3. The reliability of a channel of 0.90 provides a system value of 0.972. A channel of 0.95 gives 0.993, and a channel of 0.99 gives 0.9997.

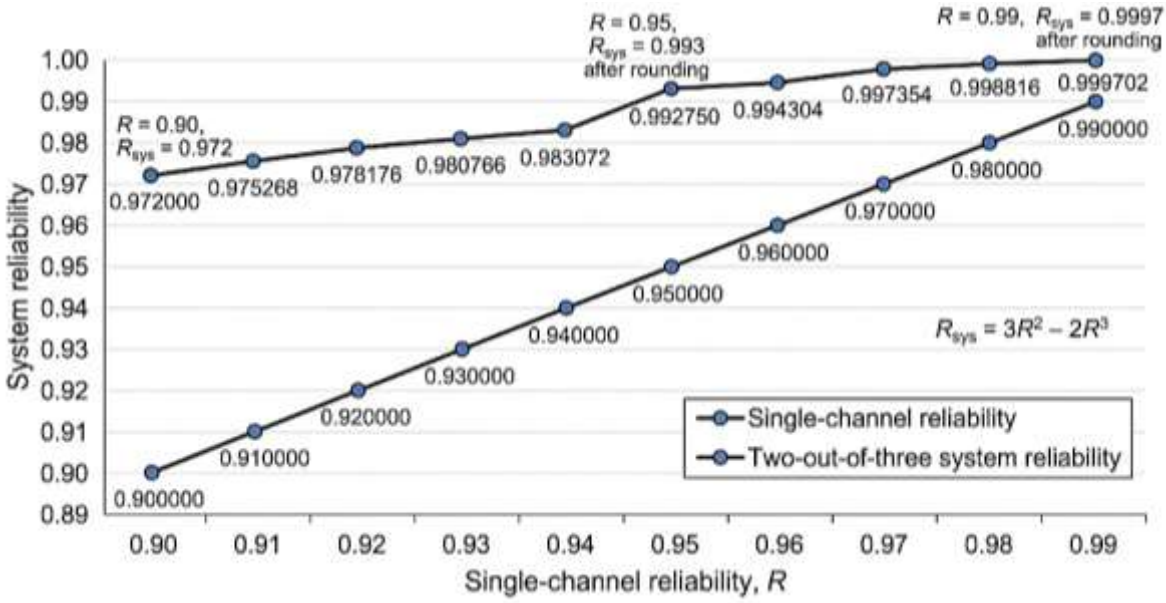


Figure 3. The channel reliability increase with a two out of three structure and a single channel structure to reliability of the system increase to 0.99

Importance sampling reduces the virtual test distance. Equation 7 presents the scale distance needed between the simulated distance and the actual distance D_{real} and the acceleration factor A.

$$D_{\text{test}} = \frac{D_{\text{real}}}{A} \tag{7}$$

In this case, D_{real} would be 20 million miles and A would be 5,000 and the distance required would be 4,000. Figure 4 illustrates the distance of factors up to 20,000. The 5,000 factor is within the range reported by Zhao and others.

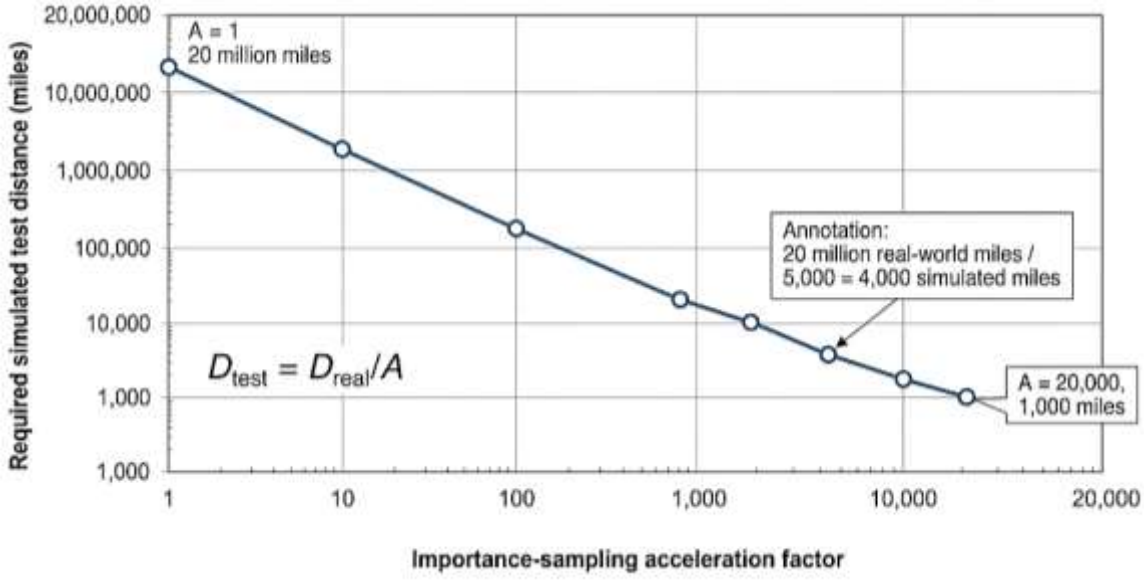


Figure 4. Distance in miles against the acceleration factor required in simulated test, 20 million, 10,000, 4,000 and 1,000 miles

RESULTS AND DISCUSSION

5.1 Readiness and Defect Detection

The chart in figure 5 indicates preparedness in the twelve builds. The coordinated arm increased by 0.52 between build 1 and build 12 to 0.93. After the fact calculation using Equation 1, the baseline scores increased from 0.50 to 0.81. Gate reviews took place at builds 3, 5, 8, 10, and 12 with thresholds of 0.60, 0.70, 0.80, 0.85, and 0.90. The coordinated arm scored 0.63, 0.74, 0.85, 0.90, and 0.93 at those builds and passed every gate. The baseline scored 0.58, 0.66, 0.75, 0.79, and 0.81 and would have failed all five. The regression arm continued to be released according to its own criteria.

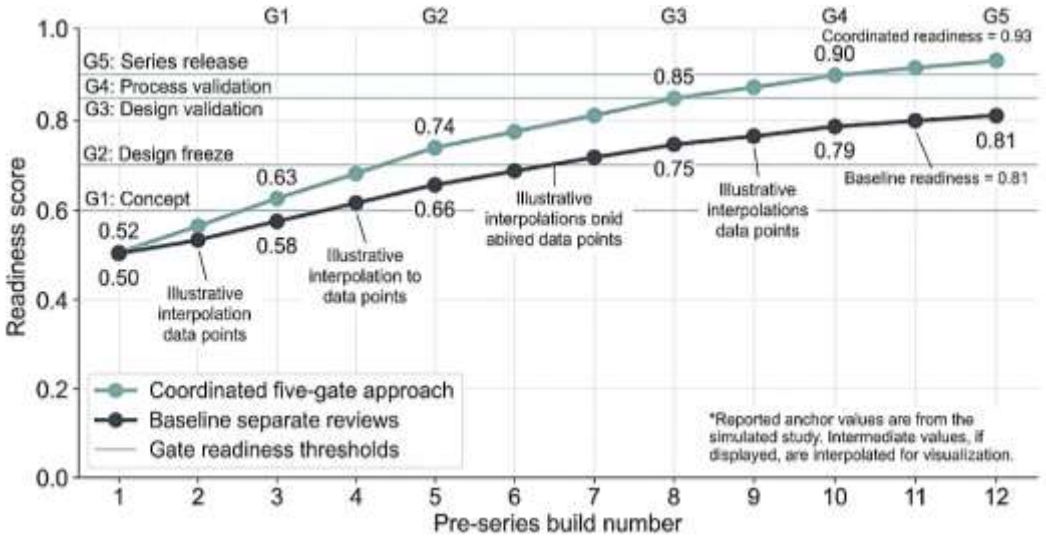


Figure 5. The coordinated arm and the baseline arm have their baseline score of readiness across all builds 1 to 12 with gate thresholds indicated

Results of the defects at each gate are reported in Table 5.

Table 5. Integration defects at each launch gate (by baseline arm and coordinated arm) that have been identified at harvest by detecting a seed, with totals and escaped.

Gate	Baseline detected	Coordinated detected
G1	5	11
G2	12	21
G3	20	25
G4	14	15
G5	6	5
Total before production	57	77
Escaped to production	27	7

The same data is presented as a chart in Figure 6. The synchronised arm detected additional defects at the initial gates. It discovered 32 defects up to G2, and the baseline discovered 17.

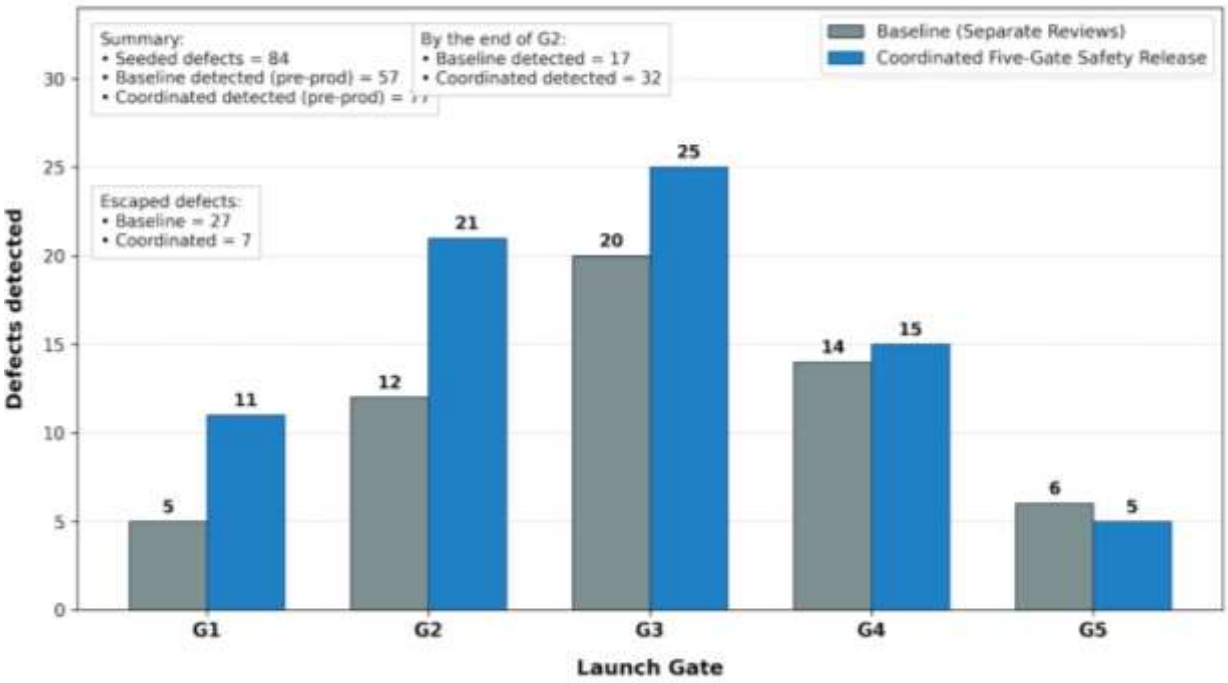


Figure 6. Defects identified at the gates G1 to G5 in baseline arm and coordinated arm.

The escape rate is given by equation 8 and represents the proportion of all defects making it into production.

$$E = \frac{D_{\text{post}}}{D_{\text{pre}} + D_{\text{post}}} \tag{8}$$

The proportion of E equals 27/84, or 32.1. The arm coordinated provides 7/84, 8.3 percent. The majority of the gain was due to timing and signal interface defects. There were also explicit acceptance criteria required with respect to learned perception inputs and to illustrate the use of qualitative and quantitative criteria a chapter on machine learning perception functions describes how admissibility of evidence can be generated and how evidence can be organised into an assurance case [24].

5.2 Occupant Protection

The sled results of the three configurations are shown in Table 6.

Table 6. The three sled configurations with occupant response which include head injury criterion, chest deflection, neck tension, head forward excursion, and the decrease in head injury criterion

Configuration	HIC15	Chest deflection (mm)	Neck tension (N)	Head excursion (mm)	HIC15 reduction (percent)
A Braking only	412	31.5	1850	188	0.0
B Late pretensioner	389	30.2	1790	171	5.6
C Coordinated pretensioner					

Figure 7 is a graph of the head injury criterion verses the full pretensioner tension lead time.

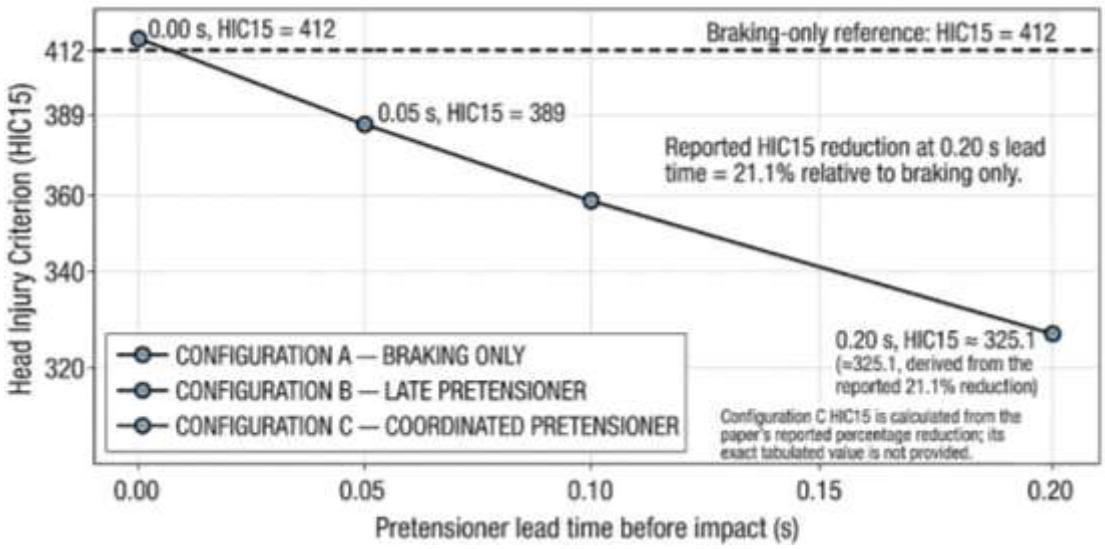


Figure 7. Criterion of head injury before pretensioner lead time of impact, with the braking of only value appearing as a reference line.

Configuration C lowered the head injury criterion by 21.1 percent compared to configuration A and head excursion was reduced by 34 percent. Configuration B gave only a small gain. This trend is consistent with previous information that pre impact braking has an effect of propelling the occupant forward and increasing the values of injuries. The advantage is time-based therefore, the common timing interface in Equation 4 is a gate item.

The coordinated gates enhanced outcomes in three ways. One readiness score discusses both product lines, meaning that the interface is rated weakly and therefore reduces the score of all. Second, the deny overrides policy prevents release in the case where one hazard remains open. Third, timing and signal defects are detected by early gates, which require evidence of the interface before the design is fixed. This trend corresponds to the demand to have a single deployment process.

The gates also have to be extended even after release. In the field, software modifications can modify the braking system or the restraint logic. Seo and others report a high assurance update system based on UN R156 and over-the-air updates to fix vulnerabilities [25]. In their work, Steger and other researchers introduce such a framework of secure and efficient software updates via wireless communication (although this time, it is on an IEEE 802.11s-based medium) as SecUp [26]. Safe and secure over the air updates Work Since design is not related to safety assurance, work on safe and secure over the air updates links update design to safety assurance [27]. According to a model-based security testing method, the attackers have the capabilities of using the update path to compromise security and safety [28]. The architecture then considers each update a micro-launch which re-executes G3 to G5 on the modified items.

The research is limited. The data are simulated and thereupon the effect sizes require field verification. These thresholds are design choices as others may require different values as indicated in Table 3. One occupant size and one crash pulse were used in the sled study. The work in the future ought to include additional occupant sizes and modes of crash and test the architecture in a real launch.

CONCLUSION

In this paper, a launch gated safety architecture was introduced that integrates ADAS into the process with occupant restraint release. Five gates, a weighted readiness score, a deny overrides decision rule, and a common timing interface are used in the architecture. The design principles of all gates were based on the review of 28 research papers. In the simulated experiment coordinated gating identified 77 of 84 seeded defects prior to production and reduced the escape rate of 32.1 percent to 8.3 percent. The Pretensioner timing led to a decrease of the head injury criterion by 21.1 percent. Avoidance and significance sampling provided evident benefits in availability and cost of the test. An extended method should include field data and post release control.

REFERENCES

[1] E. Yurtsever, J. Lambert, A. Carballo, and K. Takeda, "A survey of Autonomous Driving: Common practices and Emerging technologies," *IEEE Access*, vol. 8, pp. 58443–58469, 2020, doi: 10.1109/access.2020.2983149.

[2] P. Koopman and M. Wagner, "Autonomous Vehicle Safety: an interdisciplinary challenge," *IEEE Intell. Transp. Syst. Mag.*, vol. 9, no. 1, pp. 90–96, 2017, doi: 10.1109/mits.2016.2583491.

[3] H. Li, C. Jiang, D. Cui, S. Xie, and S. Lu, "The influences of pre-impact braking scenarios on occupant restraint system during the full frontal impact," in *Lecture Notes in Electrical Engineering*, 2017, pp. 461–468. doi: 10.1007/978-981-10-3527-2_39.

[4] S. Riedmaier, T. Ponn, D. Ludwig, B. Schick, and F. Diermeyer, "Survey on Scenario-Based Safety Assessment of Automated Vehicles," *IEEE Access*, vol. 8, pp. 87456–87477, 2020, doi: 10.1109/access.2020.2993730.

[5] U. Wilhelm, S. Ebel, and A. Weitzel, "Functional safety of driver assistance systems and ISO 26262," in *Springer eBooks*, 2015, pp. 109–131. doi: 10.1007/978-3-319-12352-3_6.

[6] M. Kölbl and S. Leue, "Automated Functional Safety analysis of automated driving systems," in *Lecture Notes in Computer Science*, 2018, pp. 35–51. doi: 10.1007/978-3-030-00244-2_3.

[7] H. Martin, K. Tschabuschnig, O. Bridal, and D. Watzenig, "Functional safety of automated driving systems: Does ISO 26262 meet the challenges?," in *Springer eBooks*, 2016, pp. 387–416. doi: 10.1007/978-3-319-31895-0_16.

[8] S. Burton, L. Gauerhof, and C. Heinzemann, "Making the case for safety of machine learning in highly automated driving," in *Lecture Notes in Computer Science*, 2017. doi: 10.1007/978-3-319-66284-8_1.

[9] S. Burton, L. Gauerhof, B. B. Sethy, I. Habli, and R. Hawkins, "Confidence Arguments for evidence of performance in machine learning for highly automated driving functions," in *Lecture Notes in Computer Science*, 2019, pp. 365–377. doi: 10.1007/978-3-030-26250-1_30.

[10] C. Hirata and S. Nadjm-Tehrani, "Combining GSN and STPA for safety arguments," in *Lecture Notes in Computer Science*, 2019, pp. 5–15. doi: 10.1007/978-3-030-26250-1_1.

[11] M. Buechel, "An automated electric vehicle prototype showing new trends in automotive architectures," in *IEEE International Conference on Intelligent Transportation Systems (ITSC)*, 2015, pp. 1274–1279. doi: 10.1109/itsc.2015.209.

[12] G. Weiß, P. Schleiß, and C. Drabek, "Fail-operational E/E architecture for highly-automated driving functions," *ATZelectronics Worldw.*, vol. 11, no. 3, pp. 16–21, 2016, doi: 10.1007/s38314-016-0032-8.

[13] D. Zhao, "Accelerated evaluation of automated vehicles safety in Lane-Change scenarios based on importance sampling techniques," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 595–607, 2016, doi: 10.1109/tits.2016.2582208.

[14] J. P. Van Marter, A. G. Dabak, A. V Mani, S. Rao, and M. Torlak, "A deep learning approach for In-Vehicle Multi-Occupant detection and classification using MMWAve Radar," *IEEE Sens. J.*, vol. 24, no. 20, pp. 33736–33750, 2024, doi: 10.1109/jsen.2024.3450432.

[15] M. Jasinski, P. Skruch, and M. Komorkiewicz, "Validation framework for generic radar sensor models," *IEEE Access*, vol. 10, pp. 18257–18267, 2022, doi: 10.1109/access.2022.3150284.

[16] F. Reway, W. Huber, and E. P. Ribeiro, "Test Methodology for Vision-Based ADAS Algorithms with an Automotive Camera-in-the-Loop," in *IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, 2018, pp. 1–7. doi: 10.1109/icves.2018.8519598.

[17] M. Elgharbawy, A. Schwarzhaupt, G. Scheike, M. Frey, and F. Gauterin, "A generic architecture of ADAS sensor fault injection for virtual tests," in *IEEE/ACS International Conference on Computer Systems and Applications (AICCSA)*, 2016, pp. 1–7. doi: 10.1109/aiccsa.2016.7945680.

[18] R. Adler, "Engineering and hardening of functional Fail-Operational architectures for highly automated driving," in

IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), 2019, pp. 30–35. doi: 10.1109/issrew.2019.00038.

[19] O. Vermesan, "Advancing the design of Fail-Operational architectures, communication modules, electronic components, and systems for future Autonomous/Automated vehicles," in *Lecture Notes in Mobility*, 2020, pp. 53–71. doi: 10.1007/978-3-030-65871-7_5.

[20] L. Capito and K. A. Redmill, "Methodology for hazard identification and Mitigation Strategies applied to an Overtaking Assistant ADAS," in *IEEE International Conference on Intelligent Transportation Systems (ITSC)*, 2021, pp. 3972–3977. doi: 10.1109/itsc48978.2021.9564820.

[21] S. Burton, "Safety assurance of machine learning for chassis control functions," in *Lecture Notes in Computer Science*, 2021, pp. 149–162. doi: 10.1007/978-3-030-83903-1_10.

[22] X. Huang, M. Kwiatkowska, S. Wang, and M. Wu, "Safety verification of deep neural networks," in *Lecture Notes in Computer Science*, 2017, pp. 3–29. doi: 10.1007/978-3-319-63387-9_1.

[23] H. Abedi, S. Luo, V. Mazumdar, M. M. Y. R. Riad, and G. Shaker, "AI-Powered In-Vehicle Passenger Monitoring using Low-Cost MM-Wave Radar," *IEEE Access*, vol. 10, pp. 18998–19012, 2021, doi: 10.1109/access.2021.3138051.

[24] S. Burton, C. Hellert, F. Hüger, M. Mock, and A. Rohatschek, "Safety assurance of machine learning for perception functions," in *Springer eBooks*, 2022. doi: 10.1007/978-3-031-01233-4_12.

[25] J. Seo, J. Kwak, and S. Kim, "Development for High-Assurance Software Update Management System complying with UN R156," *IEEE Access*, vol. 12, pp. 135811–135830, 2024, doi: 10.1109/access.2024.3426591.

[26] M. Steger, "An efficient and secure automotive wireless software update framework," *IEEE Trans. Ind. Informatics*, vol. 14, no. 5, pp. 2181–2193, 2017, doi: 10.1109/tii.2017.2776250.

[27] T. C. et al., "Safe and secure automotive Over-the-Air updates," in *Lecture Notes in Computer Science*, 2018. doi: 10.1007/978-3-319-99130-6_12.

[28] S. Mahmood, A. Fouillade, H. N. Nguyen, and S. A. Shaikh, "A Model-Based security testing approach for automotive Over-The-Air updates," in *IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, 2020, pp. 6–13. doi: 10.1109/icstw50294.2020.00019.