International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

CROSS-DOMAIN ENGINEERING GOVERNANCE FOR ADAS–RESTRAINT INTEGRATION ACROSS DESIGN, MANUFACTURING, AND QUALITY

Chethan Kanakuppe Siddegowda
ADAS Camera Engineering Development
Magna Electronics
Auburn Hills, MI, Unites States of America
Chethan.siddegowda@magna.com

Abstract

Highly developed driver assistant system and occupant restraint system are now under the umbrella of a single safety requirement, though most vehicle programs continue to deal with them in different design, manufacturing, and quality departments. This loophole allows the interface errors to go through the checks and make it to production. This paper suggests a cross-domain model of governance that creates a unified interface that receives register, end to end traceability and joint fatigue analysis, staged gates, and quality feedback involved in closed loop. The model has been tested in a Monte Carlo simulation study with 2,000 vehicle programs per three governance arms called siloed, gated, and integrated. There are 120 interface requirements between the domains of sensing, restraint control, manufacturing and quality components in each of the programs. The primary model parameters are determined by the published crash statistics and published safety engineering results. The integrated arm cut interface error varies between 22.7 and 6.0 per program and cut escaped defects of 3.68 and 0.30 per program which is 91.8 percent lower. The lead time in engineering change was reduced to 8 days compared to 21 days. Radar boresight angle, squib circuit resistance and crash sensor sensitivity process capability improved to 1.90, 1.93, and 1.59 in comparison to 1.16, 1.19 and 0.90. Elimination of end-to-end traceability created the biggest amount of benefit and escaped defects increased by 72.9 percent. The findings demonstrate the importance of a governance structure, but equally important to the technical approach in safety critical vehicle initiatives. The research provides engineering executives with an effective manner of locating gates, owners, and evidences in all the three areas. The results are based on a simulation and should be validated with program data of industry.

Index Terms—ADAS, engineering governance, occupant restraint, interface management, process capability, traceability, functional safety, cost of quality.

I. INTRODUCTION

Sensing, decision and protection have become the collaborative efforts in the area of vehicle safety. A threat is detected by a driver assistance system that plans the occupant by preparing them, and the crash energy is controlled by the structure and belts. Bengler and co-authors demonstrate how driver assistance has expanded since systems constructed on the vehicle

motion sensors like the anti-lock braking system and the stability control system to include systems constructed on radar, video and lidar systems that prevent or lessen collisions [1]. This transformation bridges the efforts of teams which used to work independently.
A study conducted by Kusano and Gabler on crash records on the rear end accidents recorded to have occurred between 1993 and 2008 of 1,396 accidents revealed that the drivers were braking in 71 percent of rear end crashes and had not braked in 29 percent of rear end crashes [2]. Their simulated vehicle systems alerted the driver of a possible crash 1.7 seconds prior to hitting something and automatic braking started 0.45 seconds before hitting anything. The combination of the systems would help to avert approximately 7.7 percent of the rear-end collisions and would reduce severe injuries by approximately half. These seconds cannot be used by a restraint system which does not obtain any information regarding the braking event.
It is not common to find an implication of this chain in organizations. The sensing algorithms and the belt hardware are owned by design teams, the different lines and test station are owned by manufacturing teams and the different audit routines are owned by quality teams. Cataldo and colleagues indicate that not only dependencies in code, but also dependencies between pieces of work are associated with the failures in software intensive products [3]. Introducing a different logic can be carried out when two safety functions share a signal but not an owner.
Standards can be of partial assistance. Koopman and Wagner believe that secure robotic vehicles require numerous disciplines to coordinate itself as a single design and implementation procedure, and mention that ISO 26262 attributes a portion of the safety responsibility to the human driver [4]. Kölbl and Leue provide that IET ISO 26262 is not a specifications document on automated driving functions [5].
This article explores the type of governance structure that maintains the ADAS and restraint integration that are right in both design and in manufacture to quality. It characterizes a cross-domain governance model, simulates the model using 2,000 programs on each governance arm and ranks the governance elements by their impact on escaped defects.

II. REVIEW WORKS

ADAS safety work is broken down into system architecture, functionality design and safety assurance work. Brännström and co-authors constructed a model using threat assessment on whether a driver could still avoid collision, through steering, braking, or accelerating, they demonstrated an improved timing of automatic braking in rear end collisions [6]. Lefèvre and co researchers sampled motion prediction, risk observation to intelligent cars that provide the danger signals that routine restraint controller may utilize [7]. Yurtsever and fellow researchers analysed typical practices in autonomous driving and demonstrated that the perception, planning and control processes are typically constructed as individual modules [8]. Paden and colleagues reviewed planning and control techniques to self-driving urban cars [9]. Ziegler and co-authors demonstrated that a vehicle that had close series sensors was capable of driving a publicly used route by itself, which drawn attention to sensor integration quality [10].
Method is the concern of safety assurance studies. Riedmaier and co-authors surveyed the scenario-based safety assessment and stated that there should be a combination of formal

verification with scenario testing, as the real traffic introduces an unlimited number of situations [11]. Burton et al. followed an assurance case format to present the issues of machine learning validation in highly automated driving, and emphasizing on perception errors [12]. Hawkins and co-authors distinguish between the safety argument, and the confidence argument, this makes quality of evidence visible [13]. Later they interrelated assurance cases to design models with a weaving model such that the cases can be written automatically [14]. Sulaman and co-authors utilized failure mode and effect analysis and system theoretic process analysis on the same forward collision avoidance system and discovered general similar results [15]. Macher et al. evaluated the approaches to threat analysis and risk assessment in the case of the automotive sector [16].

The concepts of architecture and organization expose the reason why integrating a project is unsuccessful. According to Broy and co-authors, the functions of vehicles become distributed between networked control units and require techniques that can cope with the following complexity [17]. Sangiovanni Vincentelli and Di Natale are dealing with an approach of designing distributed automotive electronics [18]. Ebert and Jones later Ebert and Favaro, record the increasing burden of embedded software on the product quality and cost [19][20]. According to Browning, there are four uses of the design structure matrix, which he referred to as component, team, activity and parameter-based forms, which aids in the break down and re-integration of the complex systems [21]. Research involving over 100 practitioners led to a conclusion by Gotel and Finkelstein that the majority of traceability issues are due to weak traceability prior to writing the requirements [22].

Table 1 summarizes the key studies, in terms of their subject matter, evidence presented, and the gap in governance that the studies leave unaddressed.

TABLE I. QUALITATIVE COMPARISON OF THE CHOSEN STUDIES BASED ON THE FOCUS, REPORTED EVIDENCE AND THE REMAINING GAP IN GOVERNANCE TO BE FILLED BY JOINTLY IMPLEMENTED ADAS AND RESTRAINT PROGRAMS.

Study	Source	Focus	Reported evidence	Governance gap for ADAS and restraint
Kusano and Gabler, 2012	[2]	Warning and braking advantage of rear end crash	1,396 crashes; approximately 7.7 percent or stopped; approximately 50 percent less serious injuries	An absence of association with time of restraint, production variation
Murmann and co-authors, 2015	[23]	Detection of crash sensor and timing of deployment	Deployment varies with severity, direction and structure, main and confirmation sensors are connected to a single diagnostic module	No connection to pre-crash ADAS data or to line testing
Koopman and Wagner,	[4]	The interdisciplinary	Redundancy reliability can be reduced by around 95 percent	Labels need to integrate but does

2017		issue of safety	through 1 billion operating hours to each catastrophe; while 1 billion catastrophes cover on diagnoses	not provide a gate model
Kölbl and Leue, 2018	[5]	Designing automated driving with a functional safety analysis	Model based method is used to compare variant of architecture with ISO 26262 principles	Halts on design and does not bother with manufacturing
Sulaman and co-authors, 2017	[15]	Comparison of method of hazard analysis	FMEA and STPA produced rather similar results with a single collision avoidance system	Fails to make the assigning of owners across domains
Hawkins and co-authors, 2011	[13]	Arguments on safety and confidence	Distinct arguments narrow-down idle evidence	Leaves out evidence of production
Browning, 2001	[21]	Design structure matrix	There are four architecture, team, activity and parameter integration matrix forms	None of the safety functions information
Gotel and Finkelstein, 1994	[22]	Requirements traceability	Research done on more than 100 practitioners; poor traceability prior to specification	None of the automotive production connections
Aggogeri and Gentili, 2005	[24]	Six Sigma of auto process capability	DMAIC was used on three types of defects in high quality automotive pipes	Not connected with safety functionalities

A general trend is presented in the table. Crash-data studies, sensing, and restraint-timing studies characterize the technical chain, and assurance, traceability and organization-studies characterize governance generally. There is no combination of these two studies and none of them is based on an interface between design purpose and completing product measurement. The gap in the model section below is addressed by the model.

III. GOVERNANCE MODEL

The model comprises of five elements. An interface register is a common interface register in which all signals, tolerance and timing values that are exiting the ADAS, restraining, manufacturing and quality domains are registered. End to end traceability connects all the item in the registers to a hazard, requirement, design feature, process control, and a test. Joint hazard analysis uses all three-failure mode and effects analysis and system theoretic process analysis, which Sulaman and co-authors found to provide similar results. Staged gates are gates which examine the register at fixed points. The closed loop quality feedback provides data on

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

production capability back to design tolerances. Fig. 1 demonstrates how all these are interrelated with the three domains.

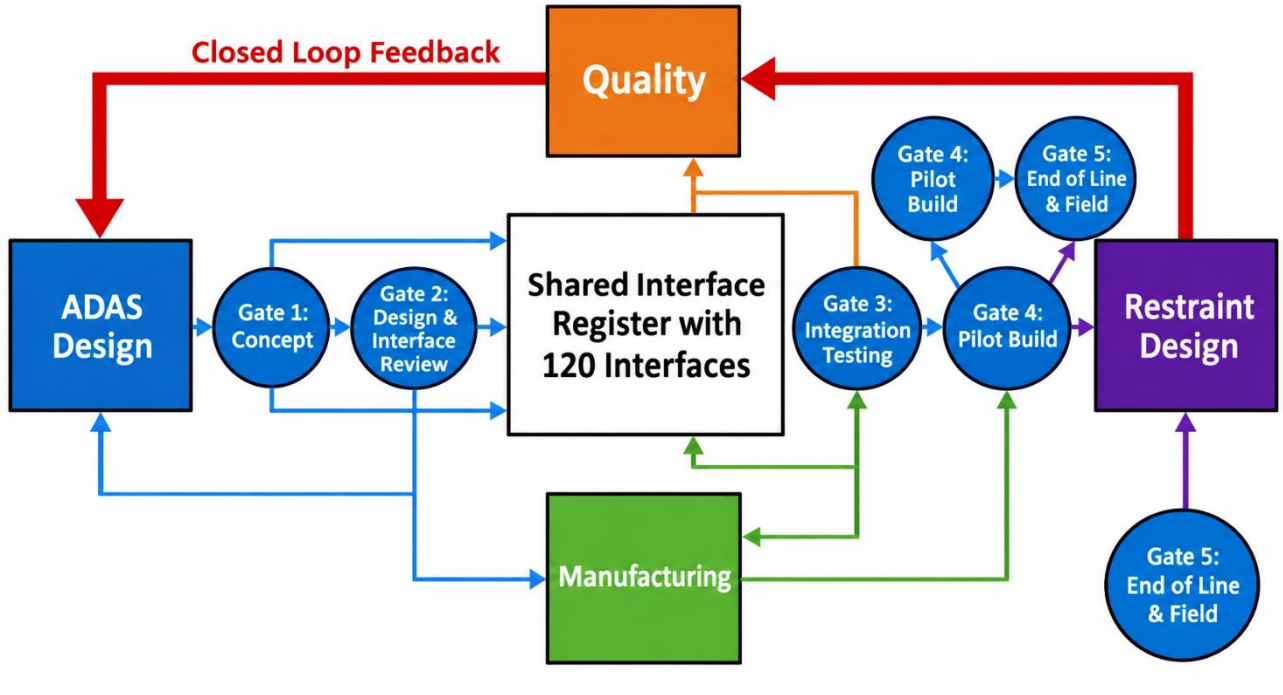


Fig. 1. Linking the ADAS design to the restraint design to manufacturing to quality via a common interface register, traceability, five gates and feedback.

The register also should contain things which cannot be described by classic requirements. Koopman and Wagner caution that machine learning functions do not lend themselves to traditional traceability between requirements and tests. The register thus contains version of data sets that have been learned in perception, along with the confidence statement about it, which Hawkins and co-authors would not want to implicate in the safety argument.

The aspect of riskiness of an interface is determined by coupling. The structure matrix of design provides a means of tallying the areas that each item is in touch with. The index of interface coupling of a program, as determined by Eq. 1, is the index of n interfaces that a program has and ck is a score between zero and one based on the proportion of domains that either write or read interface k.

$$\mathrm{ICI} = \frac{1}{n}\sum_{k=1}^{n} c_k \qquad (1)$$

The probability of interface k being mismatched upon the beginning of integration testing is provided in Eq. 2. Where m0 is the probability of base mismatch, γ is the factor of the coupling and T is the proportion of register items that are completely traceable.

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

$$m_k = m_0 \times (1 + \gamma \times c_k) \times (1 - T) \quad (2)$$

Non-detectability or transparent coupling increases the likelihood of a mismatch and traceability decreases it. The second part is supported by Gotel and Finkelstein as their research demonstrates that the issues of traceability are introduced in the early stages and propagated to the further work.

The studies created a spiral model of five gates [25]. Gate 1 checks the idea, Gate 2 analyses design and interface register. Gate 3 does integration testing. The pilot build and process approval is discussed in Gate 4. The Gate 5 includes end of line testing and early field monitoring. Every gate is a sort of fence between fault and error to failure according to Avizienis and co-authors [26].

IV. EXPERIMENTAL DESIGN

The experiment is a replica of the signal chain in Fig. 2. A threat is detected by a radar/camera. The ADAS controller provides a braking demand and warning. The restraint controller gets the request and prepares the belt pretensioner and the crash sensors afterwards confirm the crash and cause the airbag to deploy. The final step outlined by Murmann and co-authors involves main sensors and a confirmation sensor transmitting signals to a single diagnostic module that is responsible in determining whether or when and what parts of the restraints to deploy.

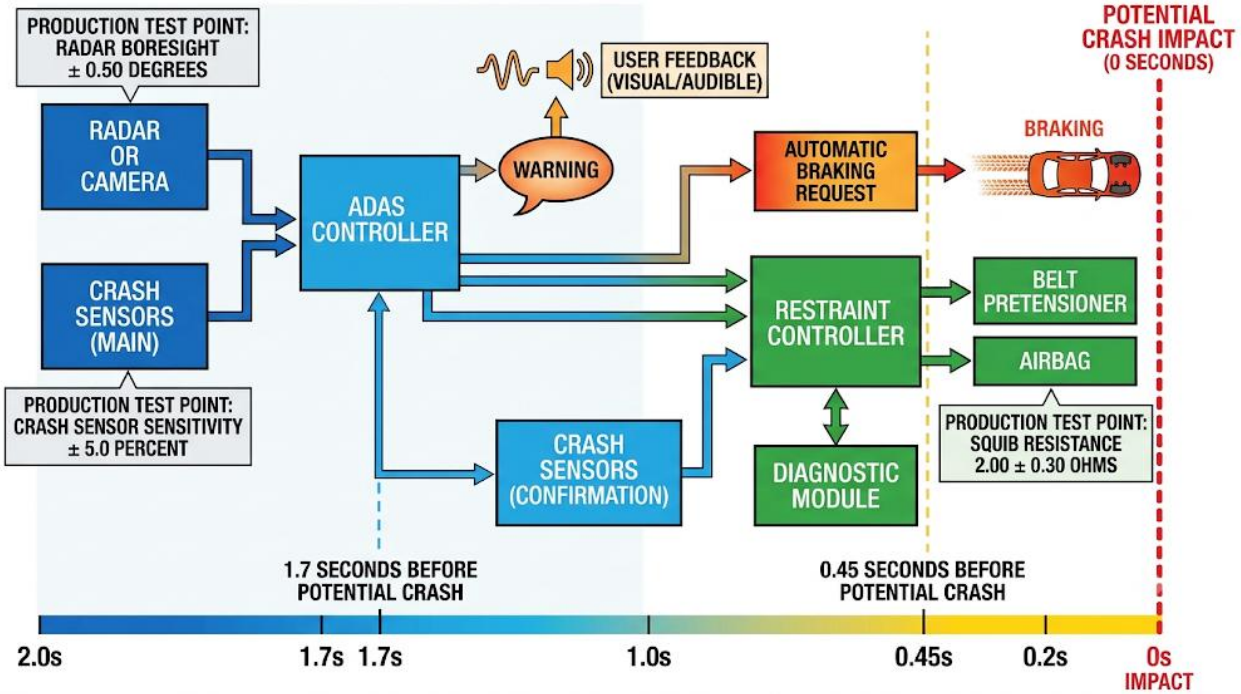


Fig. 2. Connection between threat detection and braking request/pretensioner action to crash confirmation, airbag deployment and production test points.

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

The Monte Carlo model employed in the study was done in Python. Each of the runs corresponds to one program of vehicles with 120 interface requirements. 2,000 runs were given to each arm of governance and the seed was random. The couplings weights were obtained using a beta distribution that had a mean of 0.40. Mismatches were then taken out of the Eq. 2. All gates experienced poor match with their respective characteristics, and a few emerging defects with more Poisson mean of 1.2 per program started to occur only at Gate 3 and beyond. These are the parameters listed in Table 2.

TABLE II. SIMULATION PARAMETERS OF ALL THE THREE GOVERNANCE ARMS SUCH AS TRACEABILITY, THE EFFECTIVENESS OF THE GATE, LEAD TIME, OVERHEAD AND COMMON SETTINGS.

Parameter	Siloed	Gated	Integrated
Traceability coverage T	0.55	0.75	0.88
Gate 1 effectiveness	0.15	0.25	0.32
Gate 2 effectiveness	0.30	0.40	0.52
Gate 3 effectiveness	0.45	0.55	0.62
Gate 4 effectiveness	0.35	0.45	0.55
Gate 5 effectiveness	0.30	0.35	0.45
Median change lead time (days)	21	13	8
Governance overhead (cost units)	0	90	220
Common settings	120 interfaces; m0 = 0.30; γ = 1.0; emergent defects 1.2 per program; 2,000 runs per arm	same	same

The technical parameters are determined in three sources. The 1.7 seconds warning time and the onset of the braking of 0.45 seconds comes after Kusano and Gabler. The production field presupposes networked stations streaming measurements that can be advocated by the industrial internet literature [27][28]. The production-appearing-design feedback loop takes a digital twin work [29][30].

The capability studies on three characteristics were indicator of the quality domain. The links between the ADAS sensor and the road, the restraint controller and the pretensioner, and the impact signal and the deployment decision are: radar boresight angle, squib circuit resistance, and the radar boresight angle respectively. Each characteristic produced 400 lots of 500 parts in the simulation and the lot means deviated about the nominal by an amount which varies with the arm of governance.

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

V. RESULTS

A.Detection at each gate

The probability of one mismatch to pass all the five gates is provided in Eq. 3 where eg is the efficiency of a gate g.

$$P_{esc} = \prod_{g=1}^{5}(1 - e_g) \quad (3)$$

The values of the siloed arm, the gated arm and the integrated arm are 0.149, 0.072 and 0.031 respectively. Table 3 indicates the average number of defects in each gate.

TABLE III. MEAN DEFECTS BY EACH GATE PER PROGRAM, TOTAL DEFECTS FOUND AND SHARE DEFECTS FOUND PRIOR TO INTEGRATION TESTING IN EACH ARM.

Arm	Gate 1	Gate 2	Gate 3	Gate 4	Gate 5	Total found	Found before Gate 3 (percent)
Siloed	3.39	5.84	6.61	2.81	1.59	20.24	45.6
Gated	3.13	3.75	3.78	1.40	0.60	12.66	54.3
Integrated	1.91	2.14	1.95	0.68	0.23	6.92	58.5

The same counts are in the form of a graph in Fig. 3.

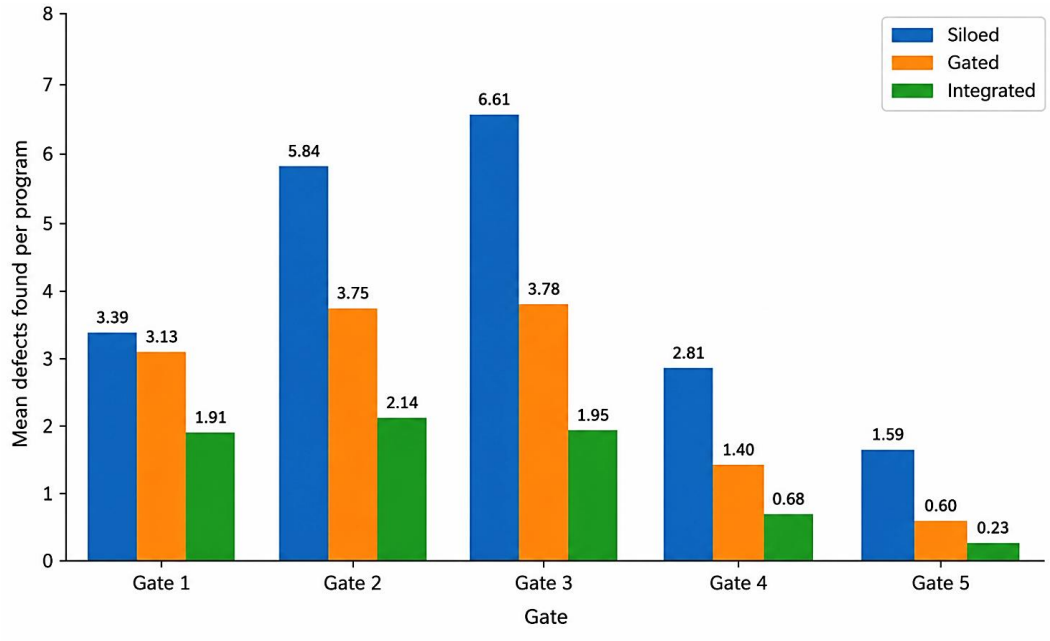


Fig. 3. Mean defects in each of five gates per program of siloed, gated and integrated governance arms.

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

The integrated arm will have less defects at each gate since there will be less defects at the beginning. It also has a greater percentage at an earlier stage 58.5 percent prior to integration testing as compared to 45.6 percent of the siloed arm. This is important since integration tests will only test a few scenarios. According to Riedmaier and colleagues, real traffic provides far too many situations to test and so the set has to be eliminated and be augmented with formal tests.

B. Escaped defects

Table 4 indicates interface mismatch and escaped defects that have 95 percent confidence intervals.

TABLE IV. MATCHES INTERFACE, ESCAPES DEFECTS INTERFACE WITH CONFIDENCE, SHARE, SHARE WITH NO ESCAPE, AND REDUCTION OF SILOED ARM PER PROGRAM.

Arm	Mismatches per program	Escaped defects per program	Programs with zero escapes (percent)	Reduction in escapes (percent)
Siloed	22.7 (22.5 to 22.9)	3.68 (3.60 to 3.77)	3.0	Baseline
Gated	12.5 (12.4 to 12.7)	1.08 (1.03 to 1.13)	34.9	70.7
Integrated	6.0 (5.9 to 6.1)	0.30 (0.28 to 0.32)	74.2	91.8

Fig. 4 indicates the distribution of escapes in the 2,000 programs in each arm.

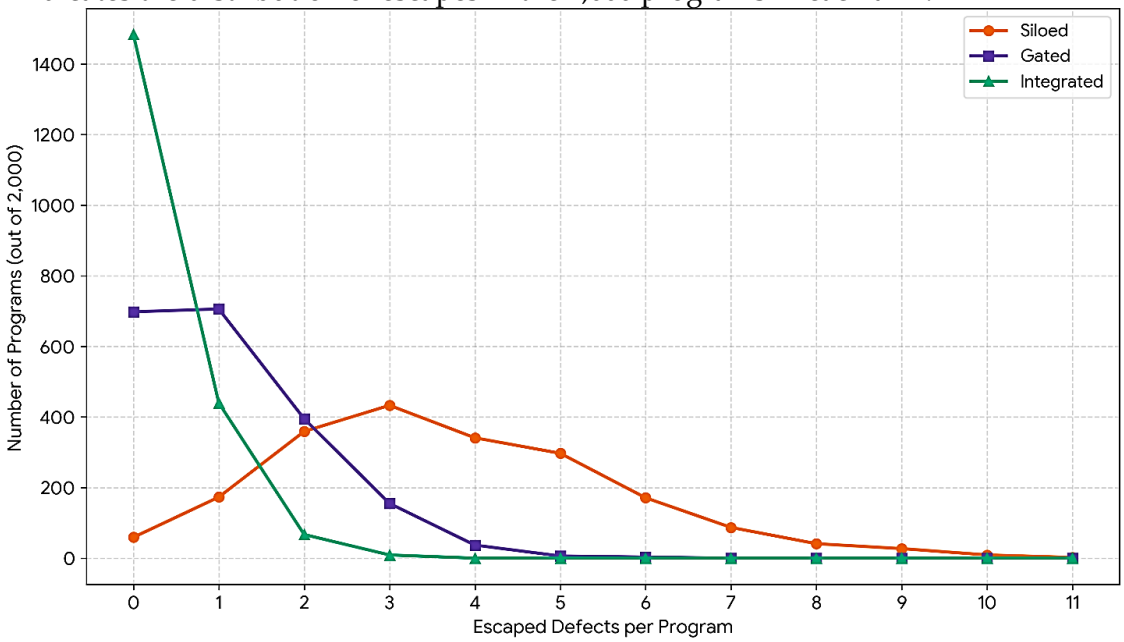


Fig. 4. Escape counts per program are distributed between 2,000 programs that are distributed across each governance arm starting at 0 escapes/program and continuing

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

The arm is siloed, and this arm (long-tailed) has 80 programs that demonstrate eight or more escapes. The integrated arm does not have more than three escapes. Koopman and Wagner demonstrate reasons why tails are important. They found that a 95-percent diagnostic coverage is sufficient to reduce reliability of a redundant automotive system in orders of magnitude with faults remaining latent. An escaped interface fault is similar to a latent fault, as it does not manifest until a crash or a braking incident occurs and causes the fault to manifest. According to Sulaman and co-authors, the two methods of hazard have an overall consensus on a system of collision avoidance, which indicates that the resulting gain is related to the construction of the structure and ownership and not a superior method.

C. Manufacturing capability

Process capability is a measure to determine the degree of a specification of a production process. The index is defined in terms of the upper and lower specification limits of the process i.e. USL and LSL, the mean of the process i.e. μ and process standard deviation i.e. σ as expressed in equation 4.

$$C_{pk} = \min\left(\frac{\mathrm{USL} - \mu}{3\sigma}, \frac{\mu - \mathrm{LSL}}{3\sigma}\right) \quad (4)$$

Aggogeri and Gentili used the DMAIC approach to a high-quality part of the vehicle and eliminated three types of defects by ensuring process control is dictated by needs of customers. The closed loop element is, as here, motivated by the same reasoning. Table 5 provides capability and anticipated out of specification parts in three characteristics providing a linkage between ADAS and restraint function.

TABLE V. THREE SAFETY CHARACTERISTICS UNDER EACH GOVERNANCE ARM, INDEX OF PROCESS CAPABILITY AND EXPECTED NUMBER OF DEFECTIVE PARTS PER MILLION.

Characteristic	Specification	Cpk siloed	Cpk gated	Cpk integrated	ppm siloed	ppm gated	ppm integrated
Radar boresight angle (degrees)	± 0.50	1.16	1.42	1.90	479	22	below 0.1
Squib circuit resistance (ohms)	2.00 ± 0.30	1.19	1.43	1.93	409	20	below 0.1
Crash sensor sensitivity (percent)	± 5.0	0.90	1.16	1.59	5,698	464	2.0

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

Fig. 5 plots the indices against the typical automotive of 1.33 against the target.

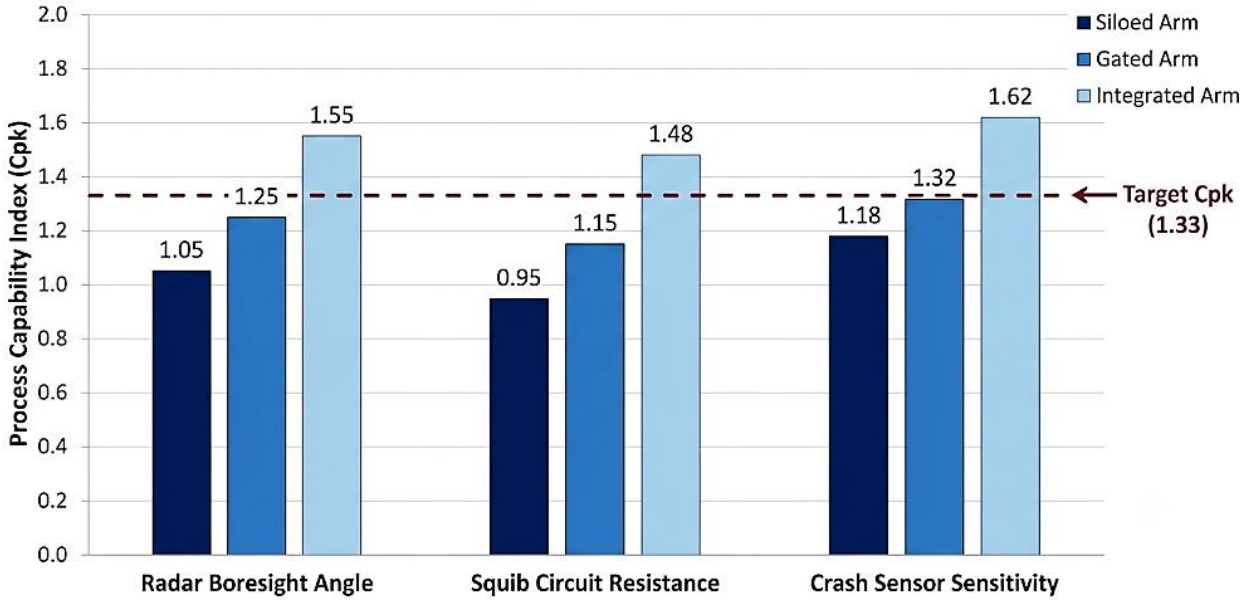


Fig. 5. Index of process capability of three safety characteristics of each governance arm with the index plotted against a target line of 1.33.

The integrated arm will only clear the target on all three characteristics. crashed sensor siloed arm has its value of 0.90, which is approximately 5,698 bad parts per million. This feature is directly related to the sensing logic Murmann et al. characterize, and thus, a negative value on this characteristic can change the deployment timing. The model has two mechanisms that contribute to the gain in capability. Variation is responded to by design tolerances and lines drift less due to faster returning of measurement data to engineers. It is this return path that is made possible by the connected sensing and digital twin tools, explained by Xu and co-authors, and Tao and co-authors.

D. Change lead time and cost of quality

The cost of quality of a single program can be described with the use of Eq. 5 where Dg is the number of defects detected at the gate g, cg is the cost of a defect correction at the gate, Desc is the number of escaped defects, cf is the cost of a field correction of a single escape, and O is the governance overhead.

$$\mathrm{CoQ} = \sum_{g=1}^{5} \left(D_g \times c_g\right) + D_{\mathrm{esc}} \times c_f + O \tag{5}$$

Stage costs were set to 1, 4, 12, 40, and 120 units, and the field cost was set to 400 units. The lead time and cost are reported in Table 6.

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

TABLE VI. CHANGE LEAD TIME, COST OF QUALITY AT CONFIDENCE LIMITS, COST INDEX VERSUS THE SILOED ARM AND OVERHEAD OF EACH ARM.

Arm	Median lead time (days)	Mean lead time (days)	90th percentile (days)	Cost of quality (units)	Cost index	Overhead (units)
Siloed	21	23.2 (22.7 to 23.7)	37.5	1,883 (1,848 to 1,918)	100.0	0
Gated	13	14.3 (14.0 to 14.5)	22.3	713 (694 to 732)	37.9	90
Integrated	8	8.5 (8.4 to 8.7)	12.5	429 (419 to 439)	22.8	220

Integrated arm reduction led to a saving of 63.3 percent in mean lead time and 77.2 percent in the cost of quality with even an overhead of 220 units paid. Cataldo et al. associate dependencies between the work items and failure as well as the fewer hand offs of the owners in a single sequence which is the shorter lead time. Browning reveals that there are such hand offs that are revealed through team-based matrices. According to Ebert and Favaro, the rapid and visible change control is becoming heavier due to the popularity of software in the guidelines of quality and development of automotive.

E. Contribution of each governance element

The integrated arm was subjected to the last test to exclude one element at a time. The result is given in Table 7.

TABLE VII. INCREASED DEFECTS PER PROGRAM SMALL RELEASE WITH CHANGE SMALL RELEASE WITH CHANGE AGAINST FULL MODEL.

Configuration	Escaped defects per program	Change against full model (percent)
Full integrated model	0.30 (0.27 to 0.32)	Baseline
Without joint FMEA and interface review	0.39 (0.36 to 0.41)	29.4
Without closed loop quality feedback	0.42 (0.40 to 0.45)	41.8
Without shared interface register	0.45 (0.42 to 0.48)	50.8
Without end-to-end traceability	0.52 (0.49 to 0.55)	72.9
Siloed baseline	3.68 (3.60 to 3.77)	1,132

The ranking is given in Fig. 6.

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

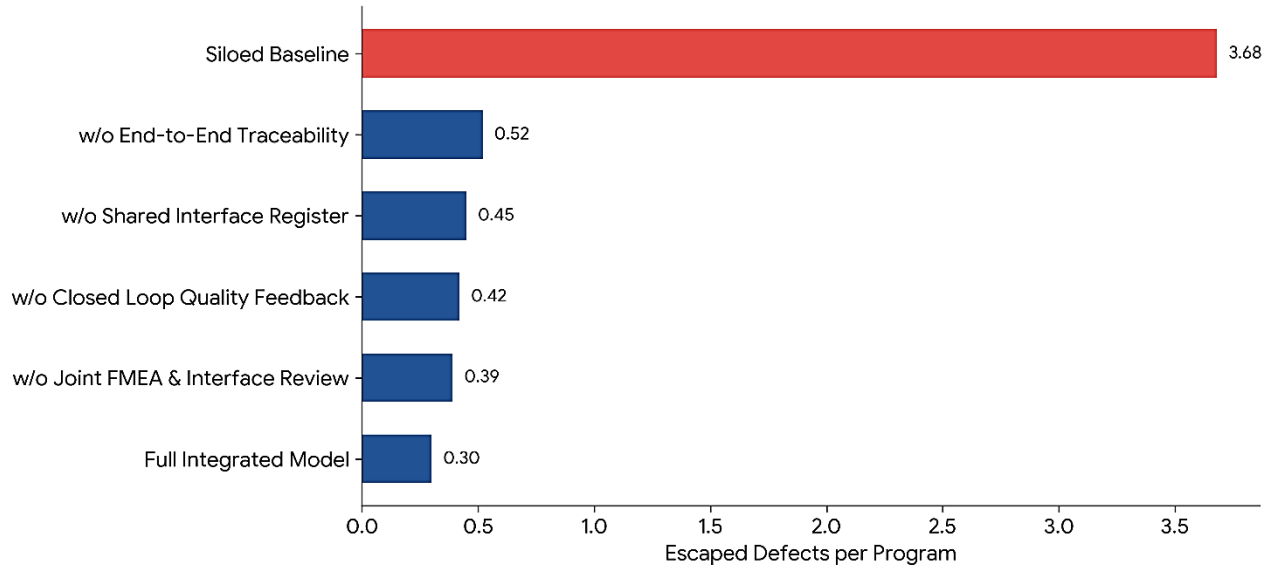


Fig. 6. The full integrated model, four element removals that are single and the siloed baseline all get enumerated as the number of defects that get escaped per program.

Traceability matters most. Its elimination increases escapes by 72.9 and shared register comes in, at 50.8. The lowest reduced setup remains 86.0 percent less than the siloed baseline. This finding indicates that there is no sole element that bears the gain and the elements connect with each other.

VI. DISCUSSION

These findings can be replicated to four rules which are practical. A single register item with a domain boundary should be owned by one named owner and the owned register item should be changeable. Second, the safety argument and a different confidence statement should be contained in every gate package, so in effect, reviewers can see the strength of the evidence. Third, model-based assurance tools need to create the case based on the design models which minimizes manual effort and drift between the design and evidence. Fourth, on a fixed schedule, there must be a recurrence of production data to design and CPK values of safety characteristics would be reviewed at Gate 4 and Gate 5.

They will require a gradual approach towards adoption. The register and traceability displayed the greatest impacts and can be initiated in a program first, then joint hazard analysis and feedback loops could be introduced on the following gate cycle. Smaller suppliers have access to register as opposed to complete model sharing, in order to keep sensitive design information confidential. A cross-domain change board must convene periodically and must have the power to halt a release in case a register item lacks evidence.

There are three more points that should be considered. Learned perception puts in data and validation evidence which normal requirements do not capture and author Burtons and others demonstrate how assurance cases are able to formalize this evidence. The signals between ADAS and restraint can also be corrupted by security faults and the ADAS review by Macher and co-authors assists the teams in their selection of risk method that suitably fits the safety process. Future designs might use restraint timing based on risk assessment outputs on the ADAS side like those sampled by Lefèvre and co-authors.

There are limitations to the study. These figures are based on a simulation and the effectiveness of the gates; the coverage of traceability and costs are all assumed figures. The model makes the gates independent, which real programs might not reflect, and it gives coupling fixed between the arms. The permutation of the arms must be valid under a wide variety of parameter regimes, but warranties, audit and production history must substantiate the size of each gain. Such records could be given by industry partners. In the future research, other gate structures and other restraint technologies, including side and curtain airbags, should also be tested due to significant differences in coupling of various types of structures in actual programs.

VII. CONCLUSION

This article outlaid a cross-domain governance framework on ADAS and restraint incorporation and experimented with a simulated 2000 vehicles programs with each governance branch. The integrated model saw asset interface mismatches decreased 22.7 per program, the escaped defects decreased by 91.8 percent, the mean change lead time decreased 63.3 percent, and the process capability on three safety characteristics rose to at least 1.59. After overhead the cost of quality decreased by 77.2 percent. Some of the shared attributes that being used to enhance were traceability, shared register, closed loop feedback on quality and joint hazard analysis but most was traceability. The results indicate that the problems posed by the integration of the safety functions are governance problems in line with the technical problems. The model should be validated with real program data in future work, and generalized to the areas of cyber security and learned perception evidence and directly tested on the dependence of their gates.

REFERENCES

1. K. Bengler, K. Dietmayer, B. Farber, M. Maurer, C. Stiller, and H. Winner, “Three Decades of Driver Assistance Systems: Review and Future Perspectives,” IEEE Intelligent Transportation Systems Magazine, vol. 6, no. 4, pp. 6–22, Jan. 2014, doi: 10.1109/mits.2014.2336271. Available: https://doi.org/10.1109/mits.2014.2336271
2. K. D. Kusano and H. C. Gabler, “Safety benefits of forward collision warning, brake assist, and autonomous braking systems in Rear-End collisions,” IEEE Transactions on Intelligent Transportation Systems, vol. 13, no. 4, pp. 1546–1555, Apr. 2012, doi: 10.1109/tits.2012.2191542. Available: https://doi.org/10.1109/tits.2012.2191542

3. M. Cataldo, A. Mockus, J. A. Roberts, and J. D. Herbsleb, "Software dependencies, work dependencies, and their impact on failures," IEEE Transactions on Software Engineering, vol. 35, no. 6, pp. 864–878, Jul. 2009, doi: 10.1109/tse.2009.42. Available: https://doi.org/10.1109/tse.2009.42
4. P. Koopman and M. Wagner, "Autonomous Vehicle Safety: an interdisciplinary challenge," IEEE Intelligent Transportation Systems Magazine, vol. 9, no. 1, pp. 90–96, Jan. 2017, doi: 10.1109/mits.2016.2583491. Available: https://doi.org/10.1109/mits.2016.2583491
5. M. Kölbl and S. Leue, "Automated Functional Safety analysis of automated driving systems," Lecture Notes in Computer Science, pp. 35–51, Jan. 2018, doi: 10.1007/978-3-030-00244-2_3. Available: https://doi.org/10.1007/978-3-030-00244-2_3
6. M. Brannstrom, E. Coelingh, and J. Sjoberg, "Model-Based threat assessment for avoiding arbitrary vehicle collisions," IEEE Transactions on Intelligent Transportation Systems, vol. 11, no. 3, pp. 658–669, May 2010, doi: 10.1109/tits.2010.2048314. Available: https://doi.org/10.1109/tits.2010.2048314
7. S. Lefèvre, D. Vasquez, and C. Laugier, "A survey on motion prediction and risk assessment for intelligent vehicles," ROBOMECH Journal, vol. 1, no. 1, p. 1, Jul. 2014, doi: 10.1186/s40648-014-0001-z. Available: https://doi.org/10.1186/s40648-014-0001-z
8. 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, Jan. 2020, doi: 10.1109/access.2020.2983149. Available: https://doi.org/10.1109/access.2020.2983149
9. B. Paden, M. Cap, S. Z. Yong, D. Yershov, and E. Frazzoli, "A survey of Motion Planning and Control Techniques for Self-Driving Urban Vehicles," IEEE Transactions on Intelligent Vehicles, vol. 1, no. 1, pp. 33–55, Mar. 2016, doi: 10.1109/tiv.2016.2578706. Available: https://doi.org/10.1109/tiv.2016.2578706
10. J. Ziegler et al., "Making Bertha Drive—An autonomous journey on a historic route," IEEE Intelligent Transportation Systems Magazine, vol. 6, no. 2, pp. 8–20, Jan. 2014, doi: 10.1109/mits.2014.2306552. Available: https://doi.org/10.1109/mits.2014.2306552
11. 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, Jan. 2020, doi: 10.1109/access.2020.2993730. Available: https://doi.org/10.1109/access.2020.2993730
12. S. Burton, L. Gauerhof, and C. Heinzemann, "Making the Case for Safety of Machine Learning in Highly Automated Driving," Lecture Notes in Computer Science, pp. 5–16, Jan. 2017, doi: 10.1007/978-3-319-66284-8_1. Available: https://doi.org/10.1007/978-3-319-66284-8_1
13. R. Hawkins, T. Kelly, J. Knight, and P. Graydon, "A New Approach to creating Clear Safety Arguments," in Springer eBooks, 2010, pp. 3–23. doi: 10.1007/978-0-85729-133-2_1. Available: https://doi.org/10.1007/978-0-85729-133-2_1
14. R. Hawkins, I. Habli, D. Kolovos, R. Paige, and T. Kelly, "Weaving an Assurance Case from Design: A Model-Based Approach," IEEE International Symposium on High

Assurance Systems Engineering (HASE), pp. 110–117, Jan. 2015, doi: 10.1109/hase.2015.25. Available: https://doi.org/10.1109/hase.2015.25

15. S. M. Sulaman, A. Beer, M. Felderer, and M. Höst, "Comparison of the FMEA and STPA safety analysis methods–a case study," Software Quality Journal, vol. 27, no. 1, pp. 349–387, Dec. 2017, doi: 10.1007/s11219-017-9396-0. Available: https://doi.org/10.1007/s11219-017-9396-0
16. G. Macher, E. Armengaud, E. Brenner, and C. Kreiner, "A review of threat analysis and risk assessment methods in the automotive context," Lecture Notes in Computer Science, pp. 130–141, Jan. 2016, doi: 10.1007/978-3-319-45477-1_11. Available: https://doi.org/10.1007/978-3-319-45477-1_11
17. M. Broy, I. H. Kruger, A. Pretschner, and C. Salzmann, "Engineering Automotive software," Proceedings of the IEEE, vol. 95, no. 2, pp. 356–373, Feb. 2007, doi: 10.1109/jproc.2006.888386. Available: https://doi.org/10.1109/jproc.2006.888386
18. Sangiovanni-Vincentelli and M. Di Natale, "Embedded system design for automotive applications," Computer, vol. 40, no. 10, pp. 42–51, Oct. 2007, doi: 10.1109/mc.2007.344. Available: https://doi.org/10.1109/mc.2007.344
19. Ebert and C. Jones, "Embedded software: facts, figures, and future," Computer, vol. 42, no. 4, pp. 42–52, Apr. 2009, doi: 10.1109/mc.2009.118. Available: https://doi.org/10.1109/mc.2009.118
20. Ebert and J. Favaro, "Automotive software," IEEE Software, vol. 34, no. 3, pp. 33–39, May 2017, doi: 10.1109/ms.2017.82. Available: https://doi.org/10.1109/ms.2017.82
21. T. R. Browning, "Applying the design structure matrix to system decomposition and integration problems: a review and new directions," IEEE Transactions on Engineering Management, vol. 48, no. 3, pp. 292–306, Jan. 2001, doi: 10.1109/17.946528. Available: https://doi.org/10.1109/17.946528
22. O. C. Z. Gotel and C. W. Finkelstein, "An analysis of the requirements traceability problem," IEEE International Requirements Engineering Conference (RE), pp. 94–101, Dec. 2002, doi: 10.1109/icre.1994.292398. Available: https://doi.org/10.1109/icre.1994.292398
23. [23] R. Murmann, L. Harzheim, and S. Dominico, "Simulation and new correlation method of crash sensor signals in misuse tests," in Proceedings, 2015, pp. 609–624. doi: 10.1007/978-3-658-08844-6_41. Available: https://doi.org/10.1007/978-3-658-08844-6_41
24. F. Aggogeri and E. Gentili, "Six Sigma Methodology: A possible solution to increase the process capability in the automotive market," in Springer eBooks, 2007, pp. 683–691. doi: 10.1007/3-211-38053-1_67. Available: https://doi.org/10.1007/3-211-38053-1_67
25. B. W. Boehm, "A spiral model of software development and enhancement," Computer, vol. 11, no. 4, pp. 14–24, Aug. 1986, doi: 10.1109/2.59. Available: https://doi.org/10.1109/2.59
26. A. Avizienis, J. -c. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11–33, Jan. 2004, doi: 10.1109/tdsc.2004.2. Available: https://doi.org/10.1109/tdsc.2004.2

27. L. Da Xu, W. He, and S. Li, "Internet of Things in Industries: A survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233–2243, Jan. 2014, doi: 10.1109/tii.2014.2300753. Available: https://doi.org/10.1109/tii.2014.2300753
28. M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The Future of Industrial Communication: Automation networks in the era of the internet of things and Industry 4.0," IEEE Industrial Electronics Magazine, vol. 11, no. 1, pp. 17–27, Mar. 2017, doi: 10.1109/mie.2017.2649104. Available: https://doi.org/10.1109/mie.2017.2649104
29. F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, "Digital twin in industry: State-of-the-Art," IEEE Transactions on Industrial Informatics, vol. 15, no. 4, pp. 2405–2415, Apr. 2019, doi: 10.1109/tii.2018.2873186. Available: https://doi.org/10.1109/tii.2018.2873186
30. Q. Qi and F. Tao, "Digital twin and big data towards smart manufacturing and industry 4.0: 360 degree comparison," IEEE Access, vol. 6, pp. 3585–3593, Jan. 2018, doi: 10.1109/access.2018.2793265. Available: https://doi.org/10.1109/access.2018.2793265