Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio

Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P528-cd

Preliminary Safety-Critical Scenario Analysis of Semi-Automated Train Operation

Yang Sun

Laboratoire Génie Industriel, CentraleSupélec, Université Paris-Saclay, France.
SNCF SA, France. E-mail : yang.sun@centralesupelec.fr

Marc Sango

SNCF SA, France. E-mail: marc.sango@sncf.fr

Anne Barros

Laboratoire Génie Industriel, CentraleSupélec, Université Paris-Saclay, France. E-mail: anne.barros@centralesupelec.fr

Guy André Boy

Laboratoire Génie Industriel, CentraleSupélec, Université Paris-Saclay, France.
ESTIA Institute of Technology, Bidart, France. E-mail: guy-andre.boy@centralesupelec.fr

France's national state-owned railway company (SNCF) plans to introduce the Automated Train Operation (ATO) system in manually operated trains to make train operations more efficient, eco-friendly, and precise. Preliminary Risk Analysis of ATO have been conducted at SNCF, but they are theoretical and have not been validated by human-in-the-loop simulation. As a contribution to the state of the art, we propose to use the PRODEC method to achieve a safety-orientated human-centered and organization-centered design, requiring the development of appropriate scenarios, which constitutes the object of this paper. To this end, our methodology and results are based on i) the analysis and categorization of the incidents that occurred within SNCF during the past years, including their classification, occurrence, and severity; ii) expert judgment. By doing so, we aim to define the human and organizational factors, as well as the technical elements that significantly impact system safety. The ten most relevant scenarios were developed.

Keywords: Railway, Risk analysis, PRODEC method, Human system integration, Scenario-based design.

1. Introduction

The railway industry is always looking for a better solution to the challenges of urbanization, safety, and climate change. Automated trains take part in global autonomous mobility. It is a more ecological solution expected to provide increased capacity and greater flexibility to the railway system. Automated Train Operation (ATO) (ERA, 2022) is a key component of future automated train. When activated, ATO can manage and supervise the traction and braking of the train according to the travel profile provided by the European Traffic Control System (ETCS). Train drivers should cooperate with the ATO over ETCS system on the next generation of automated trains. The International Association of Public Transport (UITP) has defined four levels of automation. From manual operation to fully automated train operation, we will go through the journey in several steps corresponding to the levels of automation from Grade of Automation 1 (GoA1) up to GoA4. The rail industry today is now evolving from GoA1, manual driving with cabin signaling, to GoA2, semi-automated driving with ATO. The introduction of ATO should reduce train driver’s workload, but it also raises the question of task sharing between the technological system and the train driver and how to ensure safe train operation in this cooperation framework.

The impact of automation on human operations has been discussed in several industrial fields, including railways. In aerospace, several studies have examined the possibility of applying intelligent assistance in the cockpit (Rogers, 1995); Prévôt et al., 1995; Tenney, Rogers, and Pew, 1995). In the automotive industry, driver collaboration with autonomous vehicles and automated urban transportation systems is also an emerging topic (Hakkala and Heimo, 2020; Teoh, 2020); Inagaki, 2008). These studies indicate that driver vigilance can be negatively impacted by automation. With respect to railway industry, some research has also focused on the vigilance impact of the autonomous transportation to the rail system (Spring et al., 2012); Richard, Boussif, and Paglia, 2021).

In the current literature, few work efforts are devoted to the study of safety for this semi-automated train operation. SNCF has performed some preliminary risk analysis by organizing a workgroup of experts in cognitive and railway. But the result of this work is not yet tested and validated.

This paper emphasizes the selection and construction of appropriate scenarios for further PRODEC implementations. PRODEC (Boy & Morel 2022) is a scenario-based design method that enables the elicitation of emergent properties of a human-machine system in the design phase (Carroll 1997). It is based on the development of procedural scenarios considering both existing declarative configurations, called AS-IS scenarios, and new declarative configurations to be designed, called TO-BE scenarios, run human-in-the-loop simulations, observe and analyze the various activity produced. Two kinds of comparisons are carried out: (1) comparison of AS-IS tasks and TO-BE tasks (what we call task is what is prescribed); and (2) comparison of TO-BE tasks and TO-BE activities (what we call activity is what is effectively performed). These comparisons enable the discovery of emergent properties, projecting new functions and potential infrastructure(s) that will define the projection of next TO-BE configurations of the sociotechnical systems being designed and developed.

PRODEC enables the evaluation of collaboration performances and the trust between human operators and technical systems. PRODEC is applied in several projects in different domains. A complete BPMN-CPSFA PRODEC process is produced in an air combat system in the MOHICAN project to evaluate collaboration between pilots and cognitive systems (Boy 2021). And it also contributes to the development of next-generation offshore oil-and-gas facilities that involve a fleet or robots remotely managed (Boy et al., 2023). In our scope, under the transition from manual driving trains to semi-automated trains, the question of trust and collaboration raises with the increasing automation of ATO. We identify the safety-related components in the early design phase for semi-automated trains. And by comparing the tasks in declarative knowledge and the activities elicited by Human-in-the-loops simulation under different situations, we can discover the emergent functions.

Consequently, in close cooperation with the training experts and the drivers, we decided to first analyze the existing risks on the current railway system based on accident data and choose the most critical scenarios that could guide the shift from GoA1 to GoA2.

This paper presents the analysis of open-source accident databases from SNCF, including incidents and accidents in railway structures in France from 2015 to 2022 (SNCF, 2022). Then we present the construction of the scenarios and their selection.

2. Database analysis

2.1. *Incident databases and analysis*

The French National Railway Company (SNCF) operates a large network of railways throughout France. From 2015, as part of data release policy, SNCF has begun sharing 216 databases in real-time for all types of trains and its infrastructure. These databases contain information on passenger services; the state of the infrastructure; transport flows, and rail safety. In this last category, six databases are present with 1647 elements of remarkable safety events (ESR), including incidents and accidents. An ESR is an event related to a train in service that puts itself, the other train, the passengers, or any other railway assets in danger.

Table 1. Severity scale for incidents and accidents (adapted from EPSF, (2016))

Severity	Measurable standards
1	“Minor” safety event
2	An event that could have had consequences on materials, or even slight injuries
3	An event that could have had individual human consequences (one or two seriously injured - 24 hours of hospitalization) or one person killed
4	An event that could have had collective human consequences (many seriously injured and/or several people killed)
5	An accident which had significant consequences
6	An accident which had serious consequences

French railway safety authority and its partners defined six grades of severity for incidents and accidents from minor to major (Table 1)

2.1.1. *Incidents cause categorizations*

The open-source incident database records the location, date, severity, and a short description of the incident. We first classified these incidents manually according to the incident cause. We defined two main categories: cause related to the infrastructure and rolling stocks, and violations of procedures and rules. The first category concerns technical systems failures, either rail or rolling stock. The second category includes operations that do not comply with the operational rules. Incidents in the latter category are mostly related to human errors. We define subcategories based on the role of the initiator’s occupation: train driver, signaler, and engineering worker. Table 2 presents this categorization of each incident type and its occurrences in the SNCF network from January 2015 to December 2022.

Table 2. An example of incident categorization.

Main Cause	Sub-category	Total
Technical failure	Infrastructure	374
Technical failure	Rolling Stock	150
Human Error	Train Driver	841
Human Error	Signaler	201
Human Error	Engineering workers	43

38 incidents are not included in this categorization because the incident record does not provide sufficient evidence to define the cause. These data show that more than 67% of incidents that have occurred in recent years on the SNCF network are related to human errors. Of the three roles in railway, train drivers have made the most human errors statistically. Train drivers' workload and vigilance issues during assignments are widely studied (Edkins and Pollock 1997; Naweed 2013). Despite the skills acquired, train drivers are still the main cause of incidents in the current railway system. With the introduction of ATO, the workload of train drivers and signalers is expected to be relatively reduced (Brandenburger et al. 2018). But it increases vigilance problems (Rees et al. 2017) due to the loneliness in the driving cabin and monotony of the tasks.

2.1.2. *Incidents consequences*

After this first categorization, we ranked the incidents according to their severity (consequences). The results are shown in Table 3 for the 10 most severe ones.

Table 3. An example of highest severity incidents.

Incident	Severity
Accident to person	4.89
Collision against end-of-track bumper	4.6
Collision between 2 trains rear-end	4.5
Collision against an obstacle at a level crossing	4.09
Authorization to pass a closed signal	4.0
Breakage of a piece of rolling stock	4.0
Collision against end-of-track bumper	4.0
Collision with parked or drifting vehicle	4.0
Damaged earthwork	4.0
Insufficient train brake power	4.0

The severity of the incidents is distributed between 3 and 6. The analysis shows that the most severe type of incident is Accident to person, with an average severity of 4.89. The other three types of incidents greater than 4 are: Collision against end-of-track bumper, Collision Obstruction, and Rear-end Train Collision. These incidents represent a collection of different types of collision.

The severity of the incidents is mainly distributed between 3.0 and 5.0. We divide this interval into two: [3.0,4.0) and [4.0,5.0]. 1310 incidents fall within the severity range [3.0-4.0), and 293 incidents fall within the severity range [4.0,5.0]. Fig 2 and Fig 3 show the frequency of incidents in these intervals according to the 5 cause categories. For highest and lowest severe incidents, the train driver is the cause of more than 55% of incidents on both severity intervals. Compared to the incidents in the severity range of [3.0-4.0), the failure of technical system (infrastructure and rolling stock) has a higher frequency than in the severity interval [4.0,5.0].

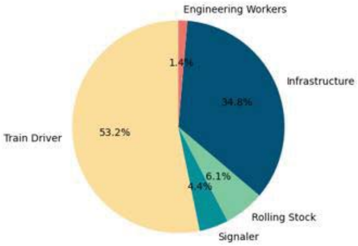


Fig. 1. Distribution of incidents in 5 categories of severity [4.0,5.0] (January 2015 to December 2022)

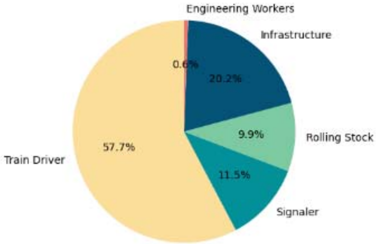


Fig. 2. Distribution of incidents in 5 categories of severity [3.0,4.0) (January 2015 to December 2022)

2.1.3. *Incidents frequency*

Serious incidents such as collisions and derailments receive a great deal of media and public attention because these incidents are often associated with significant human injury and property damage. But there are 33 incidents of severity greater than 5 during the 2015-2022 period out of 1,647 incidents. To understand the daily life and the most common incidents on the rail system, we also analyzed incidents over the past 8 years according to their highest frequency. The 10 most frequent incidents are given in Table 4.

Table 4. The 10 most frequent incidents

Incident Type	Occurrence
Inadvertent crossing of a closed signal	174
Track failure	157
Exceeding speed limit (> 40 km/h)	132
Serious signaling incident	119
Dispatch without a written speed restriction order	116
Crosses level crossing with open gates	81
Open doors in passenger trains operations	78
Derailment	75
Fire on board a train	64
Damaged earthwork	57

The results show that the most frequent incident in the French railway in recent years is the signal passed at danger (SPAD) which indicates the inadvertent crossing of a closed signal. The average severity of the incidents of this type is 3.88 which implies that the incidents can have disastrous consequence for the railway network.

A lot of research has been done on this specific incident to identify the cause (van der Flier and Schoonman 1988; Punzet, Pignata, and Rose 2018; Yan et al. 2021; Naweed et al. 2018; Kyriakidis et al. 2019). The literature shows that SPAD errors are strongly related to the train drivers' non-technical skills. According to the SPAD toolbox published by Rail Safety and Standards Board (RSSB), 91% of the SPADs are related to driver error. The most frequent causes are: "not checking the aspect of the signal", "bad reading of the signal" and "viewing the wrong signal" (RSSB 2020).

However, the train drivers are not the only ones involved in signaling errors. The signalers also play an important role in these incidents. The Serious Signaling Incident type occurred 128 times on French rail network from 2015 to 2022. This is the fourth most frequent incident among all types of incidents. The complexity of signaling control and signaling compliance make signalers and train drivers the main contributors to the incident databases. For the semi-automated trains, this situation could improve with the introduction of ATO over ETCS. On the GoA2, ATO is available to the train driver in the driver's cabin. Once the driver has activated the ATO, he or she is supposed to drive the train strictly according to the optimal braking curve calculated by the European Rail Traffic Management System (ERTMS), and all the signals must be followed accordingly.

2.2. *Expert's judgements and driver's training*

Follow-up discussions with train drivers on incidents analysis results, the train drivers noted that, from their perspective, environment around the stations is complicated and the most difficult operations part. First, the train driver must adapt the best speed to ensure a precise stop on the platform. Then he focuses on doors opening and closing at the right time to serve passengers. Weather and rail conditions are major concerns during these operations. Snow, fog, rain, and leaves on the tracks often lead train drivers to misjudge when and where to start braking. Boarding and disembarking passengers is also more difficult in these situations.

Based on these responses and the incidents analysis, we began to select the most representative scenarios from the existing ones. Our goal is always to anticipate the safety-critical elements and situations that improve the early design phase of GoA2. Thus, based on the existing scenarios, we have built corresponding scenarios on the GoA2.

3. Scenario selection and construction

A scenario describes a series of human operations and machine functionalities. Theoretical analysis of a technical system is often not human-centered or cannot be adapt to the real situation. For application at the early age of design for a future system, operational scenarios are often inspired by existing scenarios from the system's ancestor or analogous systems. In our case, to consider human behaviors and experiences in the design of a semi-automated train, we draw inspiration from existing scenarios at the SNCF training center.

From the previous incident analysis and expert interviews, we identified the conditions and events that safety-critical for current rail operations: signaling, rail conditions, and a critical safety area: the station. The SNCF training center has corresponding scenarios for manual train driving training. Among the existing training scenarios, we have selected five scenarios that can present the manual driving of a train in different situations.

The driving situation can be classified in three categories: Typical & normal situation, Critical & Abnormal situation, and Emergency & Near accident situation.

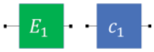
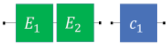
From a systemic point of view, a railway system is composed of two main parts: the environment (infrastructure, weather, etc…) and the train itself. To ensure the full functionality of the whole the environment must be suitable for train operations and the rolling stock itself must function as expected. There are different types of failures of environmental factors and onboard train systems. Based on incident analysis and expert judgment, we analyze the failure modes considering two safety related environmental elements: weather and rail obstacles. Three on board safety-related components, depending on the level of automation of the train system: at GoA1, the signalization display in the driver's cabin; at GoA2, the ETCS signalization display and the ATO. Table 5 represents the composition of the system. The system components have two states: functional or dysfunctional. The states of each component are described below.

Based on discussions with train drivers, a complete GoA1 TGV trip can be represented by the following phases: leave departure station, enter high-speed area, drive in high-speed area, leave high-speed area, enter destination station. Among these phases, the most important ones are:

- Phase 1: enter high-speed area
- Phase 2: drive in high-speed area
- Phase 3: enter in destination station.

We select and develop the scenarios during these three phases. According to the experts, the weather factor plays an important role at the station entrance. Bad weather can strongly influence train drivers' judgement of the precise position of the stop in relation to the current speed. As a result, passenger boarding and disembarking can be disrupted. This factor is only considered for the entry phase at the destination station.

Table 5. Composition of the system on GoA1 and GoA2 during three phases (normal situation)

	Manual Driving (GoA1)	Semi-automated Scenarios (GoA2)
Phase 1		
Phase 2		
Phase 3		

Environmental components:

- E_1: No obstacle on the rail
- $\overline{E_1}$: Obstacle on the rail
- E_2: Adapted weather for train operation
- $\overline{E_2}$: Bad weather for train operation

On board train components:

- GoA1:
  c_1: Signalization display fully functional
  $\overline{c_1}$: Signalization display dysfonctional
- GoA2:
  c_2: ETCS signalisation display fully functional
  $\overline{c_2}$: ETCS signalisation display dysfonctionnel
  c_3: ATO fully functional
  $\overline{c_3}$: ATO disengagement

Any presence of $\overline{E_1}$ can change a normal situation directly into emergency (e.g., $\overline{E_1}c_1$, $\overline{E_1}\overline{c_1}$, $\overline{E_1}c_2c_3$, $\overline{E_1}\overline{c_2}c_3$, $\overline{E_1}c_2\overline{c_3}$, $\overline{E_1}\overline{c_2}\overline{c_3}$, $\overline{E_1}\overline{E_2}c_1$, etc.) The train driver is always responsible for the supervision of the system function and environment perception. The obstacle on the rail can directly lead to collisions if the train driver doesn't react in time.

In our scope, component E_2 is only effective in phase 3. In both GoA1 and GoA2 contexts, scenarios of critical situation are defined by a single failure $\overline{E_2}$.

Before entering the high-speed zone, TGV panels inform the train driver that signal mode is changing. Train drivers follow the trackside signs after leaving the stations, except for TGV drivers because the high speed prevents them from doing so. Consequently, a signaling screen is available in the cabin providing a different type of activity, increasing train operations and situation awareness complexity. The safety component c_1 takes an interesting role in the entering high-speed zone phase. For manual driving on GoA1, the presence of $\overline{c_1}$ in phase 1 change the situation from normal to critical. At this phase, if the screen is not turned on automatically after passing the panels, according to the procedures SNCF, the train driver should turn on the screen manually. While the presence of $\overline{c_1}$ in phase 2 change the situation to emergency directly. During the high-speed driving, the dysfunction of signalization display makes manual driving not possible anymore. On GoA2, the signalization in cabin is a part of ETCS. ETCS controls and commands the signalization Based on its specification, various failure can potentially happen. In our research, to compare with GoA1, we only discuss the dysfunction of ETCS cabin signalization display. This dysfunction doesn't affect the functionalities of ATO. So, we can analyze these two components' failures separately. On GoA2, the situation turns to critical if there are no other failures other than $\overline{c_2}$ (e.g. $E_1\overline{c_2}c_3$).

The presence of $\overline{c_3}$ is fatal failure to the semi-automated train. In the specification, once the working conditions for ATO are not met anymore, ATO can disengage at any time of the journey. All scenarios including $\overline{c_3}$ are emergency. Under this situation, the train driver should realize as soon as possible that the ATO is no longer taking control of the train and he/she is supposed retake the brake/ traction control of the train following the signalization.

Based on these criteria, we select 5 existing scenarios on GoA1 and constructed 5 scenarios on GoA2.The scenarios are presented in Table 6.

Table 6. Example of GoA1 & GoA2 scenarios (T: typical; C: Critical; N: Normal; A: Abnormal; E: Emergency; NA: Near Accident)

	GoA1	GoA2
T & N	E_1c_1	$E_1c_2c_3$
C & A	$E_1\overline{c_1}$ (Phase 1)	$E_1\overline{c_2}c_3$
C & A	$E_1\overline{E_2}c_1$ (Phase 3)	$E_1\overline{E_2}c_2c_3$(Phase 3)
E & NA	$E_1\overline{c_1}$ (Phase 2)	$E_1c_2\overline{c_3}$
E & NA	$\overline{E_1}c_1$	$\overline{E_1}c_2c_3$

The GoA1 scenarios are existing training scenarios at SNCF. All GoA1 and GoA2 scenarios must be modeled and formalized to perform the simulations on GoA2 simulators. Before the simulation, the train drivers' tasks should be clarified and listed for each scenario. This can help us to better observe the gap between task and activity and the differences in tasks and workload on two levels of automation.

5. Conclusion and perspectives

This paper presents preliminary work for the application of the PRODEC method, the main contribution of the present work is to identify and construct declarative configurations with the most representative events and situations. The next step of this work consists in simulating the selected and constructed scenarios and configurations. The simulations will be performed on a manual driving simulator (GoA1) and a semi-automated driving simulator (GoA2). To observe the gap between activities and tasks and identify the emergent functions, we need to list tasks for each human role before the simulation.

In this paper, we use SNCF opensource database for accident analysis. This database is composed by data from different sources. The definition and accident types can differ from one institution to another. In our analysis, based on these descriptions, we resembled and recategorized several incidents to make the data more coherent.

In addition to incident analysis, a quantitative risk analysis can be applied to identify vulnerabilities and evaluate the reliability of existing barriers. Based on the results, we can validate or improve the safety procedures and better secure the semi-automated trains.

References

Boy, Guy André, Morel Chloé. 2022. "The Machine as a Partner: Human-Machine Teaming Design Using the PRODEC Method." WORK 73 (s1): S15.

Brandenburger, Niels, Anja Naumann, Birte Friedrich, and Jan Grippenkoven. 2018. "Automation in Railway Operations: Effects on Signaller and Train Driver Workload."

Carroll, John M. 1997. "Scenario-Based Design." In Handbook of Human-Computer Interaction, 383–406. Elsevier.

Edkins, Graham D., and Clare M. Pollock. 1997. "The Influence of Sustained Attention on Railway Accidents." Accident Analysis & Prevention 29 (4): 533–39.

Flier, H. van der, and W. Schoonman. 1988. "Railway Signals Passed at Danger." Applied Ergonomics 19 (2): 135–41.

Hakkala, Antti, and Olli I. Heimo. 2020. "Automobile Automation and Lifecycle: How Digitalisation and Security Issues Affect the Car as a Product and Service?" In Intelligent Systems and Applications, edited by Yaxin Bi, Rahul Bhatia, and Supriya Kapoor, 1038:121–37. Advances in Intelligent Systems and Computing. Cham: Springer International Publishing.

RSSB, 2022. "How to Use the SPAD Toolbox." n.d. Accessed February 28, 2023. http://www.rssb.co.uk/what-we-do/key-industrytopics/spad-good-practice-guide/how-to-use-the-spad-toolbox.

Inagaki, T. 2008. "Smart Collaboration between Humans and Machines Based on Mutual Understanding." Annual Reviews in Control 32 (2): 253–61.

Kyriakidis, Miltos, Samuel Simanjuntak, Sarbjeet Singh, and Arnab Majumdar. 2019. "The Indirect Costs Assessment of Railway Incidents and Their Relationship to Human Error - The Case of Signals Passed at Danger." Journal of Rail Transport Planning & Management 9 (May): 34–45.

Naweed, Anjum. 2013. "Psychological Factors for Driver Distraction and Inattention in the Australian and New Zealand Rail Industry." Accident Analysis and Prevention 60: 193–204.

Naweed, Anjum, Joshua Trigg, Steven Cloete, Phil Allan, and Todd Bentley. 2018. "Throwing Good Money after SPAD? Exploring the Cost of Signal Passed at Danger (SPAD) Incidents to Australasian Rail Organisations." Safety Science 109: 157–64.

Prévôt, T., M. Gerlach, W. Ruckdeschel, T. Wittig, and R. Onken. 1995. "Evaluation of Intelligent On-Board Pilot Assistance in In-Flight Field Trials." IFAC Proceedings Volumes 28 (15): 339–44. https://doi.org/10.1016/S1474-6670(17)45255-4.

Punzet, Lisa, Silvia Pignata, and Janette Rose. 2018. "Error Types and Potential Mitigation Strategies in Signal Passed at Danger (SPAD) Events in an Australian Rail Organisation." Safety Science 110 (December): 89–99.

Reason, James. 2016. Managing the Risks of Organizational Accidents. 1st ed. Routledge.

Rees, Amelia, Mark W. Wiggins, William S. Helton, Thomas Loveday, and David O'Hare. 2017. "The Impact of Breaks on Sustained Attention in a Simulated, Semi-Automated Train Control Task." Applied Cognitive Psychology 31 (3): 351–59.

Richard, Philippe, Abderraouf Boussif, and Christopher Paglia. 2021. "Rule-Based and Managed Safety: A Challenge for Railway Autonomous Driving Systems." In Proceedings of the 31st European Safety and Reliability Conference (ESREL 2021), 2363–69. Research Publishing Services.

Rogers, William H. 1995. "Automation Promises and Concerns for Three Levels of Automation: A Survey of Pilots of Advanced Automation Commercial Aircraft." SAE Technical Paper 951984. Warrendale, PA: SAE International.

SNCF 2022. "Incidents de sécurité (Evénements de sécurité remarquables - ESR) depuis janvier 2015." n.d. Accessed March 29, 2023.

Spring, Peter, Andrew Mcintosh, Carlo Caponecchia, and Melissa Baysari. 2012. "Level of Automation: Effects on Train Driver Vigilance." Rail Human Factors Around the World: Impacts on and of People for Successful Rail Operations, January.

Tenney, Yvette J., William H. Rogers, and Richard W. Pew. 1995. "Pilot Opinions on High Level Flight Deck Automation Issues: Toward the Development of a Design Philosophy," January. https://ntrs.nasa.gov/citations/19950021832.

Teoh, Eric R. 2020. "What's in a Name? Drivers' Perceptions of the Use of Five SAE Level 2 Driving Automation Systems." Journal of Safety Research 72 (February): 145–51.

Yan, Lu, Ying Gao, Zhiming Yuan, Hongtao Zhao, and Shigen Gao. 2021. "Robust PI Protective Tracking Control of Decentralized-power Trains with Model Uncertainties against Over-speed and Signal Passed at Danger." IET Control Theory & Applications 15 (10): 1314–34.