



CHALMERS

Chalmers Publication Library

Driver performance in the presence of adaptive cruise control related failures: Implications for safety analysis and fault tolerance

This document has been downloaded from Chalmers Publication Library (CPL). It is the author's version of a work that was accepted for publication in:

2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W) (ISSN: 2325-6648)

Citation for the published paper:

Nilsson, J. ; Strand, N. ; Falcone, P. (2013) "Driver performance in the presence of adaptive cruise control related failures: Implications for safety analysis and fault tolerance". 2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W) pp. 1-10.

<http://dx.doi.org/10.1109/DSNW.2013.6615531>

Downloaded from: <http://publications.lib.chalmers.se/publication/185006>

Notice: Changes introduced as a result of publishing processes such as copy-editing and formatting may not be reflected in this document. For a definitive version of this work, please refer to the published source. Please note that access to the published version might require a subscription.

Chalmers Publication Library (CPL) offers the possibility of retrieving research publications produced at Chalmers University of Technology. It covers all types of publications: articles, dissertations, licentiate theses, masters theses, conference papers, reports etc. Since 2006 it is the official tool for Chalmers official publication statistics. To ensure that Chalmers research results are disseminated as widely as possible, an Open Access Policy has been adopted. The CPL service is administrated and maintained by Chalmers Library.

(article starts on next page)

Driver performance in the presence of adaptive cruise control related failures: Implications for safety analysis and fault tolerance

(Invited Paper)

Josef Nilsson*, Niklas Strand[†], Paolo Falcone[‡] and Jonny Vinter*

*SP Technical Research Institute of Sweden

Box 857, SE-501 15 Borås, Sweden

Email: josef.nilsson@sp.se, jonny.vinter@sp.se

[†]VTI Swedish National Road and Transport Research Institute

Box 8077, SE-402 78 Göteborg, Sweden

Email: niklas.strand@vti.se

[‡]Department of Signals and Systems

Chalmers University of Technology, SE-412 96 Göteborg, Sweden

Email: paolo.falcone@chalmers.se

Abstract—This study explored how failures related to an adaptive cruise control (ACC) were handled by drivers and what the effects on safety can be. The experimental study included forty-eight subjects and was performed in a moving base driving simulator equipped with an ACC. Each subject experienced two different failures in separate scenarios. In total, the study included four different failures, i.e., Unwanted acceleration, Complete lack of deceleration, Partial lack of deceleration, and Speed limit violation. The outcome of each failure scenario has been categorized based on whether the driver managed to avoid a collision or not. For the outcomes where collisions were successfully avoided, the situations were analyzed in more detail and classified according to the strategy used by the driver. Besides showing that partial lack of deceleration caused more collisions than complete lack of deceleration (43% compared to 14% of the participants colliding), the results also indicate a preference among drivers to steer and change lane rather than to apply the brakes when faced with acceleration and deceleration failures. A trade off relationship was identified between allowing a failing ACC to stay operational and on the other hand disabling it when an error is detected. Keeping the system operational can cause confusion about the mode of the system but as the results of the study indicate it can also improve the situation by reducing impact speed.

Keywords—adaptive cruise control; controllability; failure model, driver behavior

I. INTRODUCTION

Adaptive cruise control (ACC) is today available in luxury as well as less expensive vehicle models. The system maintains a desired velocity while respecting a minimum time-headway (distance ahead of the vehicle given as the time it takes to travel that distance with the current velocity) to vehicles ahead by controlling throttle and brakes. Both desired velocity and time-headway are configured by the driver who is also expected to supervise the system. The driver may override the ACC using the throttle or by applying the brakes. Since the system was first release in the

1990's it has been debated whether it has a positive effect on safety or not (see for example [1] and [2]). Nevertheless, potential safety benefits of systems such as the ACC that address speed and distance keeping are relevant. Rear-end collisions represent approximately 30% of the total crashes in United States and unsafe following distance is one of the primary causation factors [3].

Independently of whether it has positive effects on safety, the ACC is a safety-related system that with its ability to command both acceleration and brake requests can cause hazardous situations [4], [5], [1], [6], [7], [3], [8], [9]. This was demonstrated in [4] where it was found that drivers had problems coping with a functional limitation preventing the ACC from considering vehicles in a stationary cue. Such a limitation is typical for ACC [7]. In the driving simulator study, presented in [4], it was found that five out of ten subjects collided with the stationary vehicles. The subjects were informed about the limitations of the ACC but anyway failed to recognize that the situation required them to take over. Another study also investigated functional limitations of an ACC in a driving simulator but instead focused on deceleration limits and degraded sensor reliability caused by rain [3]. A deceleration limit that prevents harsh braking is another typical functional limitation of the ACC. For situations where deceleration limits of the ACC (deceleration limited to $0.28g$ ($g=9.82 \text{ m/s}^2$)) prevented the system from maintaining a safe time-headway to a preceding vehicle, all sixteen drivers took over control from the ACC and avoided a rear-end collision. In rain, where degraded sensor reliability prevented the system from detecting a preceding vehicle, one of the sixteen subjects failed to take over control from the ACC and collided with the vehicle ahead. The results of these two studies ([4] and [3]) suggest that some functional limitations are handled by drivers while other are difficult for drivers to cope with.

Beside limitations in the functionality of ACC, hazardous situations can be caused by technical failures where the system does not behave according to its specification. [5] presents a driving simulator study that found that an unwanted acceleration failure caused 33% of the drivers to collide with a preceding vehicle. In another experiment, it was observed that, even though all drivers successfully handled a situation where the ACC failed to recognize a vehicle in front, they responded when the distance to the vehicle ahead was only 0.6 s on average [7]. This is below the recommended safe following distance [10]. The hazardous situations in both these studies was caused by an incorrectly applied acceleration when the ACC should have maintained a set time-headway to the preceding vehicle.

Another potential failure of ACC is to fail to decelerate the vehicle in the presence of a decelerating lead vehicle. A driving simulator study of such a scenario found that 30% of the participants collided with the vehicle in front when the ACC completely failed to slow down the vehicle [8]. Driver responses to this failure included both steering and braking with 50% depressing the brake pedal and 85% steering. Also, [8] mention that combined brake and steer responses were common in the study but they do not give precise percentages. It was suggested that reliance on the ACC both delayed and affected the type of response applied by the drivers.

The effects of reliance on automation have been recognized and analyzed before. In [11] the authors discuss the relationship between reliance and trust and the effects it can have on human monitoring of automation. Too much trust can result in overreliance on the capabilities of automation or cause humans to overlook automation failures. In this way, human trust is linked to the supervision of automation, including monitoring for functional limitations and automation failures.

As the level of automation is expected to increase in vehicles, with the ACC as one of the first systems in this development, driver supervision will be increasingly important for vehicle safety [12], [13]. Until the driver is completely removed from the task of driving it is therefore essential to understand driver responses in cases of automation failure. Efforts to deal with safety issues caused by failures of electronic systems (including ACC and other automation systems) in vehicles has led to the development and standardization of analysis methods to identify and classify possible hazards [14], [15]. These methods for analyzing hazards account for the likelihood of the driver handling the situation. This parameter of likelihood is commonly referred to as *controllability*.

The objective of our study was to explore the consequences of ACC related failures affecting acceleration and deceleration. Based on the concept of controllability we investigated if and how drivers responded to the malfunctions. Compared to the studies [5], [7], and [8] that were focused

on unwanted acceleration and complete lack of deceleration, we included those failures but also studied partial lack of deceleration. The present study also compared results over different failure modes. Related to the studies of functional limitations [4] and [3], we considered failures where system requirements were violated (i.e., ACC malfunctions). The fundamental differences being that functional limitations are known to be part of the ACC system behavior, whereas failures are unexpected events that can be prevented or tolerated but are difficult to foresee.

II. METHOD

A. Study design

A driving simulator study was designed to explore driver behavior and overall outcome for ACC related failures. The driving conditions were chosen to represent a setting for which the ACC is designed for. All driving took place within a simulated stretch of rural highway resembling a real road in Sweden. The speed limit was 110 km/h which is the typical limit on this type of road in the country. Other traffic in the same direction included faster vehicles that overtook the driver with an interval of about two minutes and slower vehicles that drove between 90 and 100 km/h. The faster overtaking vehicles were introduced to force the driver to look out for overtaking vehicles before changing lane. The slower vehicles only appeared one at a time and therefore the driver had to overtake one before the next one appeared. This setup implied that the driver experienced both the ACC control modes, speed control and distance control.

Maximum speed and time-headway could not be changed by the driver and were set to 110 km/h and 2 s, respectively. Another difference in the driver interface compared to commercial ACC systems was that the driver could not accelerate the vehicle manually, i.e., the accelerator pedal was disabled. These limitations provided the necessary bounds to ensure repeatability of scenarios for subjects without affecting the drivers ability to brake or turn off the ACC.

A fault injection tool was developed to enable failures in a situation where the driver was following a preceding vehicle at a time-headway of 2 s. Other criteria for enabling the failure were that the vehicle was positioned in the middle of the lane with a tolerance of ± 20 cm and that the driver had been driving for more than five minutes. Furthermore, to ensure that the driver experienced a fully functional ACC before the failure appeared a specially programmed lead vehicle was introduced after about six minutes. This lead vehicle drove in the right outer lane and had a velocity that oscillated between 105 and 110 km/h causing the ACC to adapt speed when following behind. If the driver tried to pass in the left lane the leader accelerated to 110 km/h and because the driver could not accelerate manually, overtaking was not possible. This configuration still did not guarantee that all drivers drove behind the specially programmed lead vehicle since they could keep trying to

overtake it. Unfortunately this meant that some drivers did not get into the follow situation and hence no failure could be introduced. These drivers are not part of the results or the analysis of this paper.

B. Participants

A total of forty-eight participants completed the experiment - thirty-three men and fifteen women between 25 and 59 years of age ($M=40.5$, $SD=9.83$). The subjects were selected from a list of people that had answered to advertisements in a local newspaper or on the VTI¹ and SP² webpages. Only persons with a self reported annual driving distance of more than 5000 km and who had held a driving license for at least 5 years were asked to participate. None of the subjects drove a vehicle with ACC on a regular basis.

In addition to the forty-eight subjects described above, another nine persons participated. Due to motion sickness or the mentioned problem of getting the subjects into the situations where failure modes could be enabled, the results of these nine persons are not considered.

C. ACC failure modes

The choice of failure modes was based on four main ways in which the ACC can malfunction, i.e., acceleration when it should not, deceleration when it should not, lack of acceleration, and lack of deceleration. From this set it was decided to focus on the most critical situations that were considered to be acceleration when it should not and lack of deceleration. Two failure modes referred to as *FM1: Unwanted acceleration* and *FM4: Speed limit violation* were devised to study accelerations when there should not be. Another two failure modes were included to study the effects of lack of deceleration, referred to as *FM2: Complete lack of deceleration* and *FM3: Partial lack of deceleration*.

For the two lack of deceleration failures (FM2 and FM3) the situation does not become critical unless there is a need to slow down the vehicle. In this study the lead vehicle therefore started to decelerate with 0.4g to a full stop at the same time as the failure was enabled. Similarly, the speed limit violation (FM4) has no effect on the behavior of the vehicle unless the preceding vehicle accelerates. The leader therefore accelerated during 28 s reaching a top speed of 150 km/h, starting at the same time as the speed limit violation failure was introduced. These changes in the behavior of the leader, together with the ACC failures contributed to create the critical situations that were the focus of this study. For unwanted acceleration (FM1), a critical situation developed even without a change in the speed of the lead vehicle.

The failure modes are described below:

FM1: Unwanted acceleration Caused the vehicle to accelerate with about 0.1g disregarding the set time-

headway. Without an intervention from the driver the vehicle collided with the leader after 10 s.

FM2: Complete lack of deceleration Caused complete inhibition of deceleration commands from the ACC. In combination with a decelerating leader this caused the time-headway to diminish, eventually ending in a collision if the driver did not intervene. The driver had a time frame of little more than 5 s to react before the vehicles collided.

FM3: Partial lack of deceleration Caused partial inhibition of deceleration commands from the ACC. In combination with a decelerating leader this caused the time-headway to diminish, eventually ending in a collision if the driver did not intervene. The driver had a time frame of between 8 to 9 s to react depending on the velocity when the failure was introduced.

FM4: Speed limit violation Caused the upper limit of 110 km/h to be disregarded and when the preceding vehicle accelerated to 150 km/h the ACC commanded an acceleration, maintaining the time-headway but disrespecting the set speed limit.

All four failure modes were only active as long as the ACC was in control. If the driver pressed the brake pedal or pushed the ACC on/off button the ACC disengaged and the failure no longer affected the vehicle. A detailed description of the functionality of the ACC is given in Section II-E2.

D. Baseline

Each failure mode was preceded by an associated baseline drive where the only difference in the scenario was that no failure was introduced. This meant that for the baseline of the FM1 scenario nothing other than the described surrounding traffic appeared during the drive. For FM2 and FM3 the leader decelerated also in the baseline scenario, the difference was that the ACC was fully functional and successfully maintained the set time-headway. In the baseline scenario for FM4 the leader accelerated to 150 km/h and the ACC correctly limited the maximum speed to 110 km/h and respected the speed limit.

The baseline scenarios were not only designed for comparing data with the failure mode scenarios, they also served to present the drivers with a fully functional ACC. The intention was to first, in the baseline scenario, present a situation where the ACC coped with the situation before the rare event of a failure occurred in the failure mode scenario.

E. Equipment

The equipment used in the study was the following.

1) *Driving Simulator*: A moving base driving simulator presenting motion, visual, and auditory cues was used in the study, see Fig. 1. The motion base of the simulator was able to perform longitudinal, lateral, and vertical linear motions as well as roll, pitch, and yaw rotational motions.

¹VTI, Swedish National Road and Transport Research Institute

²SP Technical Research Institute of Sweden

The physical workspace was ± 0.18 , ± 0.27 , and ± 0.26 meters respectively for the three linear motions. These limits prevented one to one mapping of sustained accelerations which instead were scaled down to fit within the available motion envelope. For this study it meant that even if the amplitude of accelerations had to be scaled down, the failure modes affecting acceleration still generated motion cues perceivable by the driver. Besides the motion cues for vehicle accelerations the motion base also introduced vibrations to improve the realism of the driving experience.

On top of the motion base a Volvo S80 cabin presented a realistic vehicle interface. Besides providing a driver seat, steering wheel, pedals, and instrument panel the cabin had its original left rear view mirror in place on the outside of the door. Attached to this mirror a monitor displayed the rear view in order for drivers to look out for overtaking vehicles. The simulator was not equipped with a mirror on the right side. The front view was presented on a flat canvas mounted in the position of the windscreen. With the two visual displays available to the driver it was possible to monitor surrounding traffic when failures occurred. The drivers were always driving in the right lane when the failure occurred. The lack of a right rear view mirror was therefore not considered a critical limitation.



Figure 1. The driving simulator used in the study.

2) *Adaptive Cruise Control System:* The ACC system used in this study operated from stand still and could be turned on at any speed. When there was no vehicle in front, the system operated as a speed keeping system, maintaining the set velocity of 110 km/h. If there was a vehicle in front, moving slower than the set velocity, the ACC switched to distance keeping and maintained a time-headway of 2 s.

In order to control speed and distance, the ACC issued acceleration or brake commands to a model of the simulated vehicle. To comply with the available interfaces of the vehicle model, commands were issued as engine torque or brake pedal position. Design and implementation of the ACC was therefore done as suggested in [16], with an upper- and a lower-level controller, see Fig. 2. The upper-level controller determined a desired acceleration based on radar signals (relative distance and speed compared to the

preceding vehicle) and the vehicle's own velocity. Based on desired acceleration, the lower-level controller calculates the required engine torque or brake pedal position to achieve this acceleration.

The lower-level controller had a single mode of operation whereas the upper-level controller switched between different modes depending on whether the ACC operated as a speed or distance keeping system. In the speed keeping mode a proportional-integral (PI) controller generated the acceleration commands, see Eq. 1 where a_{des}^{spd} is the desired acceleration. e_v denote the error in velocity between the desired, v_{des} , and the current, v_{own} . The proportional and integral gains, K_P and K_I respectively, were chosen to have a stable but fast system while eliminating overshoot in velocity.

$$a_{des}^{spd}(t) = K_P e_v(t) + K_I \int_0^t e_v(\tau) d\tau \quad (1)$$

where

$$e_v(t) = v_{des}(t) - v_{own}(t)$$

The distance keeping mode was an implementation based on the control law presented in [16]. The control law determines a desired acceleration given current velocity and relative distance and velocity to the vehicle in front, see Eq. 2. a_{des}^{dist} is the desired acceleration, h denote desired time-headway, and ϵ refer to the relative distance between the own and preceding vehicle measured from bumper to bumper. The parameter λ is used to tune the control law and was chosen to give stable and smooth control actions.

$$a_{des}^{dist} = -\frac{1}{h} (\dot{\epsilon} + \lambda(\epsilon + h\dot{x}_{ove})) \quad (2)$$

$$a_{des} = \min\{a_{des}^{spd}, a_{des}^{dist}\} \quad (3)$$

Finally the output of the upper-level controller was selected as the minimum of the two controllers, see Eq. 3. This simple solution caused some jerk when switching between speed and distance control but gave acceptable performance for the study.

Beside the upper- and lower-level controller the ACC also contained some logic for switching it on and off. The driver could at any time depress the brake pedal to decelerate the vehicle and at the same time disengage the ACC. A button on the steering wheel also provided a means for the driver to turn off the system. This button could also be used to reengage the ACC.

3) *Fault injection mechanisms:* The ACC was implemented as a MATLAB/Simulink [17] model. By modifying this model the system was forced into the failure modes described earlier. Fig. 3 illustrates the principal idea where a faulty signal is fed through instead of the correct when the fault enable signal is activated.

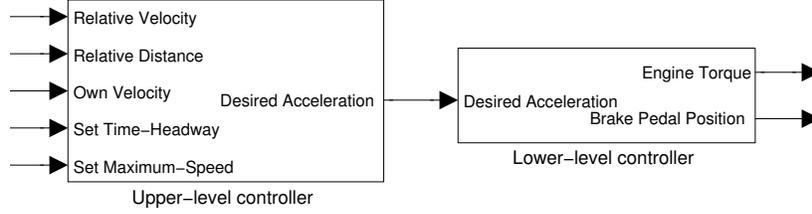


Figure 2. Model of ACC system

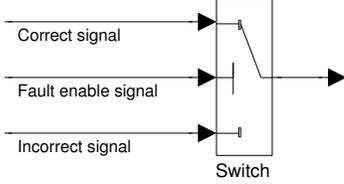


Figure 3. Fault injection block implemented in MATLAB/Simulink

Failure modes FM1, FM2, and FM3 are immediately related to the acceleration of the vehicle. These three failure modes were therefore generated by manipulating the desired acceleration signal in the interface between the upper- and lower-level controllers. Table I shows how the fault injection mechanisms are implemented. The table also describes how FM4 was generated by modifying the maximum speed setting of the ACC.

F. Procedure

On arrival the participants were welcomed and given instructions about the experiment. The instructions contained information about the procedure of the experiment and a description of the functionality of the ACC. After reading the instructions the subjects were asked to fill out a survey with background information about themselves and to sign an informed consent sheet. By signing the sheet they agreed to participate in the study but could still ask for their records to be removed at any time. Because ACC failures are generally rare, we did not reveal to the participants before the experiment that the ACC was going to fail. Instead we informed them of the true purpose of the study at the conclusion of experiment.

When the subject was seated in the simulator the experiment leader repeated some of the information from the instructions. It was stressed that the drivers should use the ACC. They were asked to act as they would in real traffic. The drivers were also shown the ACC on/off button located on the steering wheel with which they could turn off and turn on the ACC anytime while driving. They were also told that the accelerator pedal was disabled but that the brakes worked as in a normal vehicle and that by pressing the brake pedal they would disengage the ACC (if a driver disengaged the ACC before the situation with the failure had

occurred, the experiment leader asked the driver to turn the ACC back on using the ACC on/off button). After answering any questions from the participants it was time to start the practise scenario where the drivers familiarized themselves with the simulator. During the practise scenario the subjects drove with the ACC activated and were asked to explore its functionality by following as well as overtaking slower vehicles. Depending on the time it took for the participant to explore the functionality of the ACC the practice drive lasted for five to ten minutes. When finished with the practise drive the first of two pairs of baseline and failure mode scenarios was started. This way, each participant first drove one failure mode scenario preceded by its baseline scenario, followed by another failure mode scenario preceded by its baseline. The order of failure mode scenario was counterbalanced to prevent learning effects. Hence, the study included all twelve possible combinations of two out of the four failure mode scenarios. When done with all driving but before leaving, the participants were told that the true purpose of the experiment was to study their behavior in the presence of technical failures. Finally each person was rewarded with cinema tickets for their participation.

III. RESULTS

Results are presented according to failure mode. The first subsection addresses the outcome of FM1. Results of FM2 and FM3 are presented together in the second section and the third section gives the results of FM4. Beside the outcomes of the situations caused by the failure modes, results also include impact speed, minimum time-to-collision (TTC), and minimum time-headway (THW). The formulas used for calculating TTC and THW are given in Eq. 4 and 5 where v_{own} and v_{prec} are the velocities of the own and preceding vehicle and d denotes the relative distance between the two vehicles. Minimum values of TTC and THW are calculated from the time interval starting with the first appearance of the failure and ending with a collision or the successful avoidance of a collision.

$$TTC(t) = \frac{d(t)}{v_{own}(t) - v_{prec}(t)} \quad (4)$$

$$THW(t) = \frac{d(t)}{v_{own}(t)} \quad (5)$$

Failure mode	Fault injection mechanism
<i>FM1</i> Desired acceleration command from the upper-level controller is set to a constant value of 0.1g.	
<i>FM2</i> Desired acceleration command from the upper-level controller is limited to a minimum of zero, preventing deceleration.	
<i>FM3</i> Desired acceleration command from the upper-level controller is scaled down.	
<i>FM4</i> The value of the maximum speed setting is set to 150 km/h.	

Table I
DESCRIPTION OF FAILURE MODE MECHANISMS

A. *FM1: Unwanted acceleration*

Of those twenty-four drivers exposed to FM1, twenty-one successfully avoided a collision with the preceding vehicle, see Table II. One driver turned off the ACC by pressing its on/off button on the steering wheel and six drivers applied the brakes. These two types of response meant that seven subjects *slowed down* the vehicle. The remaining fourteen drivers who were successful in their actions steered and *changed lane*. None of the participants changed lane and applied the brakes simultaneously.

The drivers with an outcome classified as *aborted* in Table II lost control of the vehicle due to strong braking or steering which triggered a safety mechanism that stopped the experiment. This mechanism was implemented to prevent drivers from being exposed to unsafe excessive forces.

B. *FM2: Complete lack of deceleration and FM3: Partial lack of deceleration*

Outcomes for the situations with FM2 and FM3 are also presented in Table II. Each of these two conditions were

presented to twenty-four subjects. For both failure situations a majority of participants who avoided a collision steered and changed lane. The remaining subjects who successfully avoided a collision applied the brakes and slowed down the vehicle.

The situation in which the failure modes were enabled, as described in Section II-A, was designed to present the failures in comparable situation to all subjects. However, two participants for FM2 and three for FM3 were about to change lane when the failure was enabled. These subjects were therefore classified as *missing* and excluded from the analysis.

When the outcomes classified as missing were excluded, three out of twenty-two subjects were involved in a collision with the preceding vehicle after experiencing FM2. For FM3, nine out of twenty-one subjects collided with the preceding vehicle. Though partial loss of deceleration resulted in more collisions, the impact speed for FM3 was between 29 and 41 km/h ($M=36$, $SD=4.3$) whereas it was between 72 and 88 km/h ($M=82$, $SD=8.6$) for FM2. Other

differences between the two failure modes are the minimum TTC and minimum THW values that indicate less critical values for FM3, see Fig. 4. The differences are seen when comparing averages over all subjects, including those that collided (left side of Fig. 4), but are even more prominent when comparing minimum TTC and minimum THW for the groups of subjects who successfully avoided a collision (right side of Fig. 4).

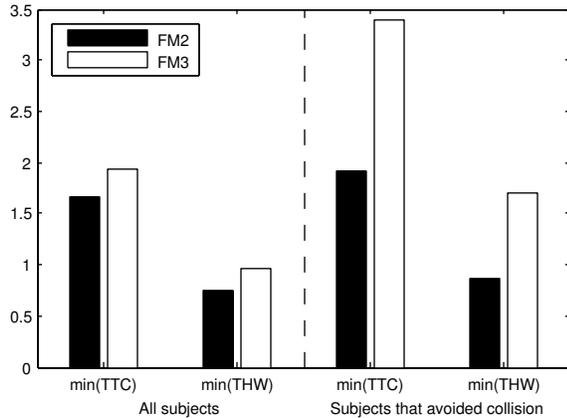


Figure 4. Average minimum time-to-collision (TTC) and average minimum time-headway (THW). Left side of the plot showing results based on all subjects (including those that collided). Right side showing results for the subjects who avoided a collision.

Because of the small number of subjects slowing down to avoid a collision it was not considered relevant to do any comparative analysis between changing lane and slowing down.

C. FM4: Speed limit violation

As Table II also shows, a majority of the drivers exposed to FM4 responded by pressing the brake pedal or turning off the ACC using its on/off button. However, eight drivers executed *no response* within 30 s after the failure had been enabled and the speed limit was violated. The response time of the drivers who did slow down was between 5.41 and 22.86 s ($M=15.44$, $SD=5.09$) measured from the time the speed first exceeded 110 km/h until the brake pedal or the on/off button was pressed.

If a driver lost control of the vehicle the experiment was aborted for the same safety reason as described for FM1, see Section III-A. Two experiments were aborted for FM4 and are classified as such in Table II.

IV. DISCUSSION AND CONCLUSIONS

We have seen that failures in the longitudinal control of the vehicle while driving with an ACC can lead to critical situations and in some scenarios the outcome is a collision. Similar results have been reported in [5] where it was found that 33% of drivers experiencing an unwanted acceleration by a failing ACC collided with a preceding

vehicle. For safety analysis and system design this implies that it cannot be expected that all drivers will cope with these technical failures. However, an interesting question for future studies is whether drivers can control failures when aided by information from a diagnostic function. In the present study, drivers were given no warnings or other indication of the failure. Had they been informed about the failure when it occurred it is expected that it would have had a positive effect on the outcome.

Besides being warned when an error is detected, drivers can be provided with continuous feedback to improve their monitoring of the automated task. Such feedback can be provided during normal as well as erroneous operation. The approach, if applied appropriately, can keep drivers alert and aware of states of the automated task that they are required to monitor [18]. Providing continuous feedback may also promote more appropriate reliance on automation. These potential benefits were studied in [19] using an interface designed to provide feedback about operation of an ACC. In their study, subjects were provided continuous values of THW and TTC in the form of a triangular or trapezoidal shape in a display. The results showed that driver responses to functional limitations can be enhanced by such feedback from an ACC.

In the present study of unwanted acceleration and lack of deceleration (FM1, FM2, and FM3) it was found that drivers steered more frequently than applied the brakes to avoid a collision. Results in [5] indicate a similar tendency where all drivers who avoided a collision steered or steered as well as applied the brakes (i.e., no driver responded with braking only). Also [8] show that steering is a common response to ACC failures. We believe that a possible contributing factor to this behavior is the separation of the driving task, i.e., that ACC controls longitudinal velocity and the driver has sole responsibility for the lateral direction. Our hypothesis is that this separation causes drivers to prefer steering rather than applying the brakes when faced with a critical situation, since brake application implies taking back control from the ACC. Furthermore, it can mean that drivers allow for some error in ACC's control of velocity and THW before intervening. This effect of automation was also demonstrated in the case of the speed limit violation (FM4), where eight drivers did nothing to slow down and the average response time of those who did slow down was more than 15 s. [20] mention similar effects, such as a diminished ability of operators of automation to detect and intervene when automation fails. They identified the effects as an out-of-the-loop problem and explained it as "loss of manual skills and loss of awareness of the state and processes of the system". [21] elaborated on related issues and mentioned the paradox of automation. Without being in direct control of a system the operator should act as a supervisor, a role that is not necessarily less demanding than manual control. Instead it requires the operator to stay vigilant even though his or

	Changed lane	Slowed down	No response	Collided	Aborted	Missing
FM1	14 (67%)	7 (33%)	-*	0 (0%)	3	0
FM2	16 (73%)	3 (14%)	-*	3 (14%)	0	2
FM3	10 (48%)	2 (10%)	-*	9 (43%)	0	3
FM4	-**	14 (64%)	8 (36%)	-***	2	0

*: Participants who did not respond were always involved in a collision. The outcome is therefore reported as a collision.
**: Not included since changing lane had not effect on the failure and little or no effect on the criticality of the situation.
***: Not applicable since the 2 s time-headway to the preceding vehicle was always maintained.

Table II
OUTCOMES OF THE FAILURE SCENARIOS (N=24 FOR EACH FAILURE)

her task is to monitor automation rather than controlling the system manually. Indications of out-of-the-loop issues were also observed in [7] where drivers responded late to an ACC failure that caused THW to gradually decrease. One explanation or contributing factor may be that drivers feel it is the ACC's responsibility to control distance and therefore they wait until the distance is critical before taking over.

A noteworthy result of the present study is that complete lack of deceleration (FM2) led to fewer collisions than partial lack of deceleration (FM3). It is believed that drivers were misled to think that the ACC was fully functional when it began to decelerate by applying the brakes. Too late the drivers realized that the applied brake force was not enough to avoid a collision. Thus, it appears that fail-silence (i.e., the ACC gives no deceleration command unless it is correct) should be required for the ACC deceleration command. Such a requirement would, according to this result improve the likelihood that drivers would successfully handle a lack of deceleration since a failure to deliver the correct deceleration command would always results in complete lack of deceleration. Support for this approach can be found in [22] and [21] where it is stated that automation should fail obviously to increase the likelihood of drivers detecting the failure. However, in the present study, it was found that both minimum TTC and minimum THW were shorter for complete lack of deceleration (FM2) compared to partial lack of deceleration (FM3) - opposite to what the number of collisions suggest. The conclusion from this finding may be that those drivers who identified the lack of deceleration were given more time to respond when the vehicle decelerated, even if it only decelerated with reduced force. With this extra time the drivers were able to keep a larger safety margin to the preceding vehicle. Together with the lower impact speed associated with partial lack of deceleration (FM3) compared to complete lack of deceleration (FM2), this suggests that the safest outcome would be achieved if drivers were made aware of the failure while the technical system decelerates as much as possible. Hence, the fail-silent failure model is not necessarily the most appropriate.

From the ACC system's perspective it could be desirable to relax a fail-silent requirement and allow some limited deviation from the completely correct output. One reason

is that feedback controllers, such as ACC, can benefit from having a failure model that takes advantage of the inherent error recovery mechanism that the feedback loop provides [23], [24], [25]. Because the controller is designed to compensate for disturbances it also proves effective in dealing with some errors in itself. The fail-bounded failure model allows the output to deviate within given bounds instead of requiring silence when an exactly correct value can not be provided, as is the case for fail-silent systems. Whether it is desirable from a driver and safety perspective to use a fail-silent or fail-bounded failure model for the ACC is the target of future work.

Follow up studies can also address limitations in the experimental setup of the present study. Like most similar studies of vehicle automation failures we used a driving simulator [5], [26], [8]. Experiments in simulators are safe and reproducible but can lack realism since the environment presented to the driver is artificially generated. Replicating studies in different simulators adds confidence in results but provide no proof of correspondence with real-world driving. Future work should therefore replicate the present study in other driving simulators but also look at alternatives such as conducting experimenters on a test track. The limitations of test track experiments are not negligible but together with driving simulator studies they can provide a broader view of the consequences of ACC related failures.

Another limitation of the present study was the disabled accelerator pedal. Commercially available ACC systems typically allow the driver to override the ACC and request additional acceleration. It is possible that this limitation affected the drivers and that they would have responded differently in the failure scenarios if they had been able to accelerate using the pedal. However, using the pedal as a response to the ACC failures would have worsen the situations and does not seam to be a reasonable action from drivers. Another potential effect of the disabled accelerator pedal may have been that drivers felt less included in the task of controlling speed than they do with a typical ACC. As a consequence they may have been more likely to steer and change lane than to apply the brakes and slow down when the ACC failed.

ACKNOWLEDGMENT

This work has been carried out in association with SAFER - Vehicle and Traffic Safety Centre at Chalmers, Sweden. The authors would like to acknowledge Prof. MariAnne Karlsson at Chalmers University of Technology and Dr. Lena Nilsson at VTI Swedish National Road and Transport Research Institute for valuable input during all phases of this study.

REFERENCES

- [1] M. Hoedemaeker and K. A. Brookhuis, "Behavioural adaptation to driving with an adaptive cruise control (ACC)," *Transportation Research Part F: Traffic Psychology and Behaviour*, vol. 1, no. 2, pp. 95–106, Dec. 1998.
- [2] A. Vahidi and A. Eskandarian, "Research advances in intelligent collision avoidance and adaptive cruise control," *IEEE Transactions on Intelligent Transportation Systems*, vol. 4, no. 3, pp. 143–153, 2003.
- [3] B. D. Seppelt, M. N. Lees, and J. D. Lee, "Driver Distraction and Reliance: Adaptive Cruise Control in the Context of Sensor Reliability and Algorithm Limits," in *Proc. Third International Driving Symposium on Human Factors in Driver Assessment, Training and Vehicle Design*, Rockport, ME, 2005, pp. 255–261.
- [4] L. Nilsson, "Safety effects of adaptive cruise controls in critical traffic situations," in *'Steps Forward'. Proceedings of the Second World Congress on Intelligent Transport Systems '95 Yokohama*, Tokyo, 1995, pp. 1254–1259.
- [5] N. A. Stanton, M. Young, and B. McCaulder, "Drive-by-wire: The case of driver workload and reclaiming control with adaptive cruise control," *Safety Science*, vol. 27, no. 2-3, pp. 149–159, 1997.
- [6] N. A. Stanton, M. S. Young, G. H. Walker, H. Turner, and S. Randle, "Automating the Driver's Control Tasks," *International Journal of Cognitive Ergonomics*, vol. 5, no. 3, pp. 221–236, Sep. 2001.
- [7] C. M. Rudin-Brown and H. A. Parker, "Behavioural adaptation to adaptive cruise control (ACC): implications for preventive strategies," *Transportation Research Part F: Traffic Psychology and Behaviour*, vol. 7, no. 2, pp. 59–76, 2004.
- [8] J. Park, D. Sung, and W.-S. Lee, "A Driving Simulator Study on Adaptive Cruise Control Failure," in *Proc. SICE-ICASE 2006 International Joint Conference*, Busan, 2006, pp. 2138–2141.
- [9] W. Spiessl and H. Hussmann, "Assessing error recognition in automated driving," *IET Intelligent Transport Systems*, vol. 5, no. 2, p. 103, 2011.
- [10] K. Vogel, "A comparison of headway and time to collision as safety indicators," *Accident Analysis & Prevention*, vol. 35, no. 3, pp. 427–433, May 2003.
- [11] R. Parasuraman and V. Riley, "Humans and Automation: Use, Misuse, Disuse, Abuse," *Human Factors*, vol. 39, no. 2, pp. 230–253, 1997.
- [12] F. Flemisch, A. Schieben, N. Schoemig, M. Strauss, S. Lueke, and A. Heyden, "Design of Human Computer Interfaces for Highly Automated Vehicles in the EU-Project HAVEit," in *Universal Access in Human-Computer Interaction. Context Diversity*, C. Stephanidis, Ed. Berlin, Heidelberg: Springer, 2011, vol. 6767, pp. 270–279.
- [13] T. Hesse, J. Engström, E. Johansson, G. Varalda, M. Brockmann, A. Rambaldini, N. Fricke, F. Flemisch, F. Köster, and L. Kanstrup, "Towards User-Centred Development of Integrated Information, Warning, and Intervention Strategies for Multiple ADAS in the EU Project interactIVe," in *Universal Access in Human-Computer Interaction. Context Diversity*, C. Stephanidis, Ed. Berlin: Springer, 2011, vol. 6767, pp. 280–289.
- [14] MISRA, *Guidelines for safety analysis of vehicle based programmable systems*. Warwickshire, UK: MIRA Limited, 2007.
- [15] ISO (International Organization for Standardization), "ISO 26262: Road vehicles - Functional safety," 2011.
- [16] R. Rajamani, *Vehicle Dynamics and Control*, ser. Mechanical Engineering Series, F. F. Ling, Ed. New York: Springer-Verlag, 2006.
- [17] MathWorks, "MATLAB/Simulink," May 2013. [Online]. Available: <http://www.mathworks.se/products/simulink/>
- [18] D. A. Norman, "The 'Problem' with Automation: Inappropriate Feedback and Interaction, not 'Over-Automation'," *Philosophical Transactions of the Royal Society B: Biological Sciences*, vol. 327, no. 1241, pp. 585–593, Apr. 1990.
- [19] B. D. Seppelt and J. D. Lee, "Making adaptive cruise control (ACC) limits visible," *International Journal of Human-Computer Studies*, vol. 65, no. 3, pp. 192–205, 2007.
- [20] M. R. Endsley and E. O. Kiris, "The Out-of-the-Loop Performance Problem and Level of Control in Automation," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 37, no. 2, pp. 381–394, 1995.
- [21] L. Bainbridge, "Ironies of automation," *Automatica*, vol. 19, no. 6, pp. 775–779, 1983.
- [22] C. E. Billings, "Human-Centered Aircraft Automation; A Concept and Guidelines (NASA Tech. Memorandum 103885)," NASA Ames Research Center, Moffett, CA, Tech. Rep., 1991.
- [23] J. Cunha, R. Maia, M. Rela, and J. Silva, "A study of failure models in feedback control systems," in *Proc. International Conference on Dependable Systems and Networks*, Göteborg, 2001, pp. 314–323.
- [24] J. Vinter, A. Johansson, P. Folkesson, and J. Karlsson, "On the design of robust integrators for fail-bounded control systems," in *Proc. 2003 International Conference On Dependable Systems And Networks*. San Francisco, CA: IEEE, 2003, pp. 415–424.
- [25] M. Gäfvert, B. Wittenmark, and O. Askerdal, "On the effect of transient data-errors in controller implementations," in *Proc. 2003 American Control Conference*, Denver, 2003, pp. 3411–3416.

- [26] D. de Waard, M. van der Hulst, M. Hoedemaeker, and K. A. Brookhuis, "Driver Behavior in an Emergency Situation in the Automated Highway System," *Transportation Human Factors*, vol. 1, no. 1, pp. 67–82, 1999.