Safe and Secure Platooning of Automated Guided Vehicles in Industry 4.0

Muhammad Atif Javed\(^a\), Faiz Ul Muram\(^b,c\), Sasikumar Punnekkat\(^b\), Hans Hansson\(^a,b\)

\(^a\)RISE Research Institutes of Sweden, Västerås, Sweden
\(^b\)School of Innovation, Design and Engineering, Mälardalen University, Västerås, Sweden
\(^c\)Department of Computer Science and Media Technology, Linnaeus University, Växjö, Sweden

Abstract

Automated Guided Vehicles (AGVs) are widely used for materials transportation. Operating them in a platooned manner has the potential to improve safety, security and efficiency, control overall traffic flow and reduce resource usage. However, the published studies on platooning focus mainly on the design of technical solutions in the context of automotive domain. In this paper we focus on a largely unexplored theme of platooning in production sites transformed to the Industry 4.0, with the aim of providing safety and security assurances. We present an overall approach for a fault- and threat tolerant platooning for materials transportation in production environments. Our functional use cases include the platoon control for collision avoidance, data acquisition and processing by considering range, and connectivity with fog and cloud levels. To perform the safety and security analyses, the Hazard and Operability (HAZOP) and Threat and Operability (THROP) techniques are used. Based on the results obtained from them, the safety and security requirements are derived for the identification and prevention/mitigation of potential platooning hazards, threats and vulnerabilities. The assurance cases are constructed to show the acceptable safety and security of materials transportation using AGV platooning. We leveraged a simulation-based digital twin for performing the verification and validation as well as finetuning of the platooning strategy. Simulation data is gathered from digital twin to monitor platoon operations, identify unexpected or incorrect behaviour, evaluate the potential implications, trigger control actions to resolve them, and continuously update assurance cases. The applicability of the AGV platooning is demonstrated in the context of a quarry site.

Keywords: AGVs, Safety, Security, Assurance Cases, Platooning, Dynamic Risk Management, Industry 4.0

1. Introduction

There is an increasing trend of Automated Guided Vehicles (AGVs) and platooning. AGVs are an integral part of the Industry 4.0 [1]. Their platooning tends to improve overall safety, security and operational efficiency of production site. The published studies on platooning focus mainly on the design of technical solutions of automotive domain, but not considered the AGV platooning in production sites and Industry 4.0. This paper presents a platooning strategy which not only provides a means to control overall traffic flow at production site and reduce resource usage but also manage transportation risks in a dynamic manner. However, the automation, digitalisation and connectivity of AGVs with each other or with the infrastructure significantly pose the safety and security issues [1, 2]. For instance, an AGV in the platoon shared the information with other AGVs, which in turn use this data for making decisions. A security attack or a single failure in one AGV could lead to unsafe behaviour of whole platoon that can potentially harm humans (injuries or even deaths) or create damages to machines, property or the environment. The safety-critical systems can only be regarded as safe if they are also secure. Besides the safety, the security should be built into the design [3]. The hazard analysis provides the basis for safety, in particular, the identification of hazards and their causes, mechanisms for elimination or mitigation. The security analysis targets the identification of potential threats and vulnerabilities and developing the mechanisms to avoid, control, or otherwise mitigate those causes, which may result in financial, privacy, safety or operational loss.

The literature highlights a dearth of comprehensive research on different aspects of vehicle platooning including safety and security analyses [4]. There is a need for comprehensive studies to deal with the situations such as joining and leaving platoon in production sites, connectivity with fog and cloud servers, system or component failures, security attacks, and influencing environmental factors. The research in [5] investigates the ISO 26262 standard from a cooperative system perspective using a platoon scenario. It includes all vehicles that are part of the cooperative functionality in the safety lifecycle. To accommodate the highest severity, an additional severity class is required, and as a consequence Automotive Safety Integrity Level (ASIL) E is suggested. Mizuma and Nakamura [6] target the bus platoon and uses IEC 61508 together with Fault Tree Analysis (FTA) for its safety evaluation. The assurance cases are used to demonstrate the acceptable safety and security of the system. The research in [7] considered the design and assurance case patterns for car platooning. However, design-time safety and security assurance are not enough for AGV platoon-
ing. Failure cases during the operational phase often lead to invalidation of documented assurance cases, thus necessitating some means for dynamic assurance. Safety and security assurance in the context of platoons in any generic context is a wide-open research domain. Due to the recent focus on Industry 4.0, platooning of AGVs becomes extremely relevant as well as provides a manageable context within confined operational areas and comparatively lesser threats landscape. Such a well-defined, though somewhat restricted setting, provides an important basis for further exploring combined safety and security assurance of platooning.

This paper focuses on the AGV platooning in Industry 4.0, where our specific contributions are: a) platooning strategy for materials transportation in gated construction sites b) applying established safety and security analyses methods c) assurance cases for demonstrating acceptable safety and security and d) resolving deviations in intended platooning behaviour caused by hazards and attacks during the operational phase. We now provide an overview of the steps in our approach.

- First, a platoon strategy is presented for materials transportation in production sites based on Industry 4.0. To carry out the data driven transportation and operations management, the architectural levels of the things, fog and cloud are considered.

- Second, the Hazard and Operability (HAZOP) and Threat and Operability (THROP) techniques are used to identify potential platooning hazards, threats and vulnerabilities. Similar to the former, the latter is carried out using guide words, but it focuses on threats rather than hazards. Based on the results gained from applying HAZOP and THROP, the safety and security requirements are derived to prevent or mitigate the impacts of hazards and attacks. The assurance cases are constructed to demonstrate the acceptable safety and security, by providing comprehensive, logical and defensible justification of the safety and security of AGVs in predefined platooning environments. The work presented in this paper utilises the Goal Structuring Notation (GSN) [8] for modelling and visualizing the assurance (safety and security) cases.

- Third, the platooning strategy is implemented in the Volvo CE simulation-based digital twins. The safety, security and flexibility is not just enhanced through AGVs interactions, but also achieving a fog-centred control scheme. Even if the safety and security analyses are performed during design and development phase, the operational changes may still adversely impact the platoon safety, security and performance.

- Finally, to carry out the dynamic risk management, the operational data is used, in particularly for identifying, monitoring, evaluating and resolving deviations from specified behaviours. The gaps in assurance cases are also resolved to avoid the culture of paper safety and security at the expense of actual system safety and security assurance.

The usefulness of the proposed AGV platooning approach is exemplified for the construction equipment domain, using the scenario of a quarry site, which solely produce stone and/or gravel products in various dimensions.

The rest of this paper is organized as follows: Section 2 describes essential background information on: (i) materials transportation and data flow in Industry 4.0, (ii) hazard and threat analyses, and (iii) assurance cases. Section 3 presents the proposed approach for safe and secure platooning of AGVs. Section 4 demonstrates its applicability for a quarry site production scenario. Section 5 discusses the related work. Section 6 concludes the paper and presents future research directions.

2. Background

2.1. Materials Transportation and Data Flow in Industry 4.0

Industry 4.0 is based on four design principles: interoperability, information transparency, technical assistance and decentralized decisions [9]. Interoperability targets the data exchange by exploiting the Internet-of-Things (IoT). This provides a means for collaborative operations. Information transparency is enabled through virtual equivalents, such as simulation-based digital twins (i.e. fusion of the physical and virtual worlds) can be leveraged for accessing real-time information and improving productivity [9, 10]. Technical assistance is provided for understanding and controlling events, for example, the comprehensive visualizations facilitate humans to solve the problems in short time frames. Decentralized decisions intend to support automatic decision making so that the human intervention is not required, which makes the operator rather a supervisor.

The generic architecture of Industry 4.0 consists of three levels: things, fog and cloud. The things, such as AGVs and robots are inter-connected physical objects equipped with sensors, actuators and controllers. Fog server/controller represents the local computation and communication capability close to the things. To carry out the transportation and distribution of materials in Industry 4.0, the AGVs are selected. They interact with one another, and to the fog that, in-turn, interact with the cloud infrastructure. The cloud is a remote infrastructure typically owned by a third-party service provider. As the things have limited storage and processing power, they rely on the fog or cloud. In addition, the control actions can be commanded through fog that acts as a bridge; it receives data from the things and perform partial processing, or otherwise forward the data to the cloud infrastructure. Such an architecture assumes real-time fault free transfer of messages (related to control, status and data) to ensure correct functioning of the system.

2.2. Hazard and Threat Analyses

To make the vehicles platoon safer, along with the hazard analysis, there is need to perform threat analysis. In particular, hazard analysis process deals with the identification of hazards, their causal factors and specification of safety goals/requirements with the intention to eliminate or mitigate the hazard risks [11], whereas threat analysis refers to the identification of potential threats and attacks, mapping of the
threats with the security attributes and specification of security goals [3]. In this paper, HAZOP and THROP techniques are used to perform hazard analysis and threat analysis, respectively. The HAZOP analysis has been successfully used for the identification of hazards in safety-critical system-of-systems [12]. In our works, although a detailed hazard analysis is performed for the system-of-systems production in quarry site, but reduced results are presented for specific focus areas like AGV platooning in this paper. For supporting the dynamic reconfiguration, we performed the hazard analysis by explicitly considering the modularity, scalability, diagnoseability, customizability, convertibility and integrability characteristics [13]. THROP analysis was previously applied for managing security risks of autonomous systems with drones [14].

HAZOP analysis is preferably carried out in the design and development phase taking different system components/parts into consideration, such as software, hardware, procedures, human error and environment. The HAZOP analysis process starts with a full description of a system, which is broken down into system parameters/functions, such as software data flow, voltage, start-up and shutdown [11]. Next, all possible deviations from intended behaviour are systematically identified by comparing a set of guide words (e.g., no, more, less, and other than, etc.) against a list of parameters of a system (e.g., location, voltage and software, etc.). For each deviation, an assessment is carried out to decide whether the deviation could occur, and if so whether the consequences of particular deviation can have negative effects on the system’s operation. Finally, appropriate recommendations that can help to prevent accidents and reduce exposure are identified. THROP is derived from the HAZOP method to identify threats relevant to the feature rather than potential hazards [3]. The THROP analysis technique also applies guide words to the given system architecture or primary functionality of a feature to identify unconsidered deviations (e.g., unexpected functionality, unwanted connection, etc.) of the system. Threat analysis by using THROP technique is performed to find out whether the potential risks of the threats are high enough to cause serious accidents, if yes then proper countermeasures are identified to eliminate or mitigate them.

2.3. Assurance Cases

An assurance (safety and security) case is a collection of auditable claims, safety and/or security arguments, and evidence created to support the claim that a defined system, service or organisation will operate as intended for a defined application in a defined environment [8, 15]. There are several ways to document assurance cases, e.g., free text, tabular structures and graphical notations. The Structured Assurance Case Metamodel (SACM) [15] is the Object Management Group (OMG) standard that integrates and standardizes the broadly used notations for documenting assurance cases, including GSN and Claims-Arguments-Evidence (CAE). The work presented in this paper utilises the PolarSys OpenCert tool platform for modelling and visualising assurance (safety and security) cases. OpenCert is an open source tool for process, assurance and certification management; its argumentation editor is based on the GSN graphical notation [16]. However, Common Assurance and Certification Metamodel (CACM) implemented in OpenCert internally uses the SACM metamodel.

<table>
<thead>
<tr>
<th>(Goal Identifier)</th>
<th>(Context Identifier)</th>
<th>(Strategy Identifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>{Goal Identifier}</td>
<td>{Context Identifier}</td>
<td>{Strategy Identifier}</td>
</tr>
<tr>
<td>&lt;Goal Statement&gt;</td>
<td>&lt;Context Statement&gt;</td>
<td>&lt;Strategy Statement&gt;</td>
</tr>
</tbody>
</table>

Figure 1: GSN Notations

The main objective of a tree-oriented goal structure is to show how a larger or main goal (claim in CACM/SACM) is broken down into one or more sub-claims until supported by solutions (evidences in CACM/SACM). The evidence can be obtained from non-formal sources, e.g., performed hazard analysis and used simulations or from formal verification, e.g., the results of model checking [17, 18]. Strategy or argument reasoning describes a rationale for decomposing the goals into sub-goals, whereas context expresses the scope, domain and operational environment in which the goals or strategy are stated. Justification element is a supporting argument that provides an explanation why a certain goal or strategy is considered acceptable. Assumption element presents an explicit statement that contributes to the comprehensiveness of an argument (i.e., a certain goal or strategy is assumed to be true).

The argument elements can be linked with one of the two relationships: SupportedBy and InContextOf. The SupportedBy relationship is used to show the inferential or evidential relationships between elements. In particular, inferential relationship ( AssertedInference in CACM/SACM) describes that there is an inference between goals in the argument, whereas evidential relationship ( AssertedEvidence in CACM/SACM) presents the connection between a goal and the solution. InContextOf ( AssertedContext in CACM/SACM) relationship is used to present contextual relationships of goals or strategy with context, assumption and justification elements. GSN extended the SACM, for instance, undeveloped and uninstantiated decorators can be applied to the elements those need to be further developed and to be replaced (instantiated) with a more concrete instance, respectively. An away goal referenced to a claim presented in another argument module. For further details we refer the interested reader to GSN standard [8].

3. Safe and Secure Platooning in Industry 4.0

System safety is an overarching process that begins during the earliest phase of a system design and continues throughout
its entire life cycle. In the context of automated and connected systems, such as AGVs, the alignment of safety with security is crucial, since any threat or attack either directly or indirectly on an AGV could lead to potential safety losses, such as human injuries or even deaths, create damages to machines, property or the environment. As per the SAE J3061 standard [3], the security process of road vehicles needs to be tailored in conjunction with the ISO 26262 standard [19]. In addition to the safety, in this paper, we address security aspects during the system design rather than adding it at the end of development, which can lead to incorrect, incomplete and unnecessary security controls and additional vulnerabilities.

The proposed approach for the development and maintenance of AGVs platoon is shown in Figure 2, which comprises of four phases. At the outset, the functional use cases of AGV platooning strategy are identified and defined (see Section 3.1). These include AGV data acquisition and processing for movement control, communication and connectivity with other AGVs and fog controller, travelling to target site locations, collision avoidance in circumstances of failures, attacks and environmental factors, etc. The functional use cases provide a basis for conducting the safety and security analyses during design and development phase. The first, second and third rows of safety and security analyses phase correspond to the hazard and threat identification, risk assessment and risk control, respectively. In particular, we applied the HAZOP and THROP techniques to identify hazards and threats. The risk assessment is carried out with the aim of evaluating the causes of identified hazards and threats, assessing severity and the probability of occurrence. Afterwards, the risk control is conducted that focuses on the establishment of mechanisms to prevent or mitigate the consequences of potential hazards and threats, derivation of safety and security requirements, and documentation of assurance cases to demonstrate the acceptable safety and security of the system (see Section 3.2).

In the third phase, to depict the structure, behaviour and interactions of AGVs platooning, the simulation-based digital twins are leveraged (see Section 3.3). This not only increase the confidence, but also serve as a resource to find additional hazards and threats. In the last phase, the dynamic safety and security assurance is carried out during operational phase. In particular, simulation data is gathered to monitor platoon operations, identify unexpected or incorrect behaviour, evaluate the potential implications and trigger control actions to resolve them, and update the assurance cases (see Section 3.4).

3.1. Functional Use Cases

The AGVs are equipped with sensors, actuators and controllers. For the perception of environment, raw data from sensors is acquired and processed. The AGV communication component is responsible for receiving and sending commands to other AGVs and fog controller that, in-turn, interact with the cloud infrastructure. Figure 3 shows platooning strategy in production sites and Industry 4.0. In circumstances the obstacle distance is less than the minimum distance, the speed is accordingly adapted. In particularly, the slow down in far range and stopping in close range is commanded. AGVs operate in both isolation and conjunction. Operating AGVs in a platooned manner provide means for efficient movement control. Often, the movement of AGVs is only permitted in autonomous operating zones and the entry of manual vehicles and humans is forbidden in this zone due to safety reasons. The zones permissions can be dynamically changed during operation [20].

In the production contexts, besides joining of AGVs in a platoon for travel between zones, to carry out individual operations, the leaving of platoon is commanded. The individual vehicle commands such as queue, pause and exit [20] are sent to egoAGVManager. The rear AGV maintains its position in the
spot previously used by front AGV. The research in Muram et al. [12] depicts the interactions of autonomous haulers/AGVs with other machines used in the quarry production site, such as excavator, mobile primary crusher, wheel loader and secondary crusher. After the completion of individual operations such as loading and unloading, the AGV moves at a slow speed towards target and wait for followers; speed is matched before pair/join them in a platoon. To avoid the collision, besides reducing speed of rear AGV, the speed of front AGV is increased when required. Chauffer is responsible for safe and secure platoon operations. To safely travel towards destination, the AGVs need to maintain their position along the path. In the platoon mode, the AGVs collect and use information from the rear and front AGV. For example, the desired speed and steering angle in a point in time are sent from front to rear AGVs and used for positioning along the path. The AGVs with certain problems, such as low battery and brake failure are removed from the platoon. In circumstances the braking distance is increased due to environmental factors, the tracking distance is accordingly increased. Typically, the leader is first AGV. When the AGV platoon is completed, the higher speed is maintained. Besides the AGVs that are regarded as things, the fog and cloud levels are used [1]. Instead of all the AGVs, the fog server controls the movement of AGV platoon by giving commands to the leader. The fog directly instruct to the things, but the cloud forwards commands to the things/AGVs via fog servers. The fog server further transmits the failure events to the cloud. The interested reader may refer to our previous work [1] for further details on mapping to the generic architecture of Industry 4.0.

3.2. Safety and Security Analyses

This subsection describes the safety and security analyses during design and development phase for AGV platooning. The safety analysis revolves around the hazards, for which a detailed hazard analysis is performed on the highest risk hazards to identify controls or safety mechanisms that eliminate or mitigate the consequences of hazards. Likewise, in the security analysis process, a detailed threat analysis is performed on high risk identified threats to identify security controls and reduce the likelihood of a successful attack. In this paper, HAZOP is selected to perform the hazard analysis, whereas THROP is applied to perform the threat analysis. The AGV platooning strategy described in Section 3.1 is used as input for performing HAZOP and THROP analyses. The functions and behaviour of individual system or components (e.g., AGV communication, Ego AGV manager, motion manager, etc.) as well as their interactions are considered. The fog controller monitors and controls the movement of AGV platoon. In case hazards and threats are encountered, fog gives the command to leader AGV, which forwards the commands to other AGVs in a platoon. The outcomes of hazard and threat analyses are used for the derivation of safety and security requirements, and documentation of assurance cases that provide appropriate arguments and evidence.
to support safety and security claims. The derived requirements and appropriate measures are used for designing and configuring the simulation environment, which serves as a digital twin.

The HAZOP and THROP analyses are conducted through a series of meetings. The personnel have a thorough knowledge of the analysis process as well as system safety and security concepts. The group discussions were conducted to establish guide words and their interpretations, and system parameters, functions or components to ensure that the AGV platooning is explored in every conceivable manner. After many discussions, a list of guide words (e.g., no/not, false/true, incorrect, increase/exceed, unavailable, unintended, exploit, other than, etc.) and systems parameters/functions, such as sensors (e.g., camera, LiDAR, speed and wheel encoder), actuators (e.g., accelerator, brake, and steering), communication and connectivity (e.g., WiFi, V2V, V2F), distances (tracking and current), locations, travel paths, and type of messages (e.g., request, response, and command) are selected for evaluation. The deviations are identified by comparing each system parameter/function to a list of key guide words, i.e., systematically questioning how deviations may occur. Afterwards, an assessment is carried out to discover all possible causes (more or less obvious ways) of deviations. Then, the risks of the potential hazards and threats are measured through a combination of severity (e.g., catastrophic, critical, marginal and negligible) and probability (e.g., frequent, probable, occasional, etc.). If the risk value is higher and non-tolerable then recommendations or countermeasures are determined to avoid, control, or otherwise mitigate the risk. However, if the risks are tolerable they could be ignored during operation. The HAZOP and THROP worksheets are established to record the hazard and threat analyses results.

3.2.1. HAZOP Analysis

Table 1 shows a few results selected from the AGV platooning hazard analysis report. The Item column in Table 1 is used to provide a unique identifier of each high-risk hazards. In platoon malfunctioning behaviour of a single AGV may affect multiple AGVs and potentially cause hazardous situations that are significantly more severe than the consequences of a single AGV failure. Let’s consider H_S1 item, a brake system that controls the deceleration of an AGV to avoid collisions. The brake system performance is not only dependent on the condition and effectiveness of the brake components, but also reaction time to activate the brakes and road conditions. The H_S1 item is related to the deviation that occurs due to degradation of braking system performance, caused by broken motor, loss of power or fluid leakage. The critical incidents can occur if an AGV is driving at high speed in the platoon to manage the safe distance from the front AGV and the ego AGV applied brake to reduce the current speed that fails to deliver the requested braking torque or not working properly. The failure of braking system may lead to the collision of AGVs. The collision can be catastrophic, especially if the AGV carries dangerous materials (e.g., explosive, toxic, etc.). This can be prevented by using auxiliary brake system sufficiently at the right time and by sending status information to leader and rear AGVs. In addition, the rear AGV will take the decision based on its onboard sensors and information received from leader AGV and other AGVs (distance, acceleration and speed) through vehicle to vehicle (V2V) communication.

There is a possibility that AGV speed sensor emits wrong values or Global Positioning System (GPS) receiver estimates incorrect location (see H_S2 item). AGV with only local/ego sensors information might lead to lateral and longitudinal instability and unsafe behaviour of the platoon. This can be mitigated by getting the relative speed and distances of front and rear AGVs and absolute location and tracking speed information from leader through AGV communication. Based on these variables the correct desired speed, acceleration and missing data will be calculated or estimated. It can be seen from the hazard analysis results that the performance of obstacle detection and collision avoidance mechanism (see H_S3 item) may be affected for which the reasons include the degradation of LiDAR (Light Detection and Ranging) or cameras. As a consequence, the collision with other obstacles (e.g., human, and machine) may happen, which could be avoided if AGV takes the decision (e.g., desired speed and steering) based on the received information from the leader and front AGVs through V2V communication and motion manager, as well as ego wheel speed sensor measurements. The power or electrical system failure (see H_S4 item) caused by short circuit inside ego AGV, which in turn lead to collision of AGVs in platoon, machine damage or major environmental damage. The control measure that could solve this problem is that rear AGV will take the decision based on its on-board sensors and send information to leader AGV. The fog controller gives the command to leader, which forwards the commands to faulty AGV to leave the platoon, and/or rear AGV to rotate the steering wheel to prevent mishap risk.

3.2.2. THROP Analysis

In this paper, we focused on the safety-related attacks that relates to critical situations, such as interference in AGV platoon movements and collision. Table 2 shows the reduced threat analysis results from the THROP worksheet, in which communication, sensors data, steering and braking functions are taken into consideration. It can be seen from the THROP results that an unauthorised individual or attacker masquerades as a legitimate member (impersonate) of AGV platooning to access the communication network (see T_S1 item). Then the attacker can use the legal identity to send malicious message to target AGVs. In spoofing or message falsification an attacker acts as a platoon leader or member that can manipulate one AGV to send erroneous messages to other AGVs. In particular, spoofing, impersonation and masquerading can send false information, such as incorrect speed, acceleration and distance, apply brake or rotate steering to other AGVs. This might lead to unintended movement of an AGV and unsafe behaviour of the platoon, for example, leaving platoon, changing lane and entrance of AGV in restricted area, and collision of AGV with other machines or human. As a control measure, vulnerability scan could be performed, message authentication scheme (e.g., digital signatures, hash-based message authentication code) would be applied to prevent from masquerading, spoofing, and imperson-
Degradation of braking system performance, fails to deliver the requested torque  

Broken motor, loss of power, fluid leakage  

The collision of AGV with other machines or human worker may happen; loss of critical hardware and human injuries or life loss  

AGV should use auxiliary brake system sufficiently at early/right time and send status information to leader and rear AGVs; the rear AGVs will take decision based on its on-board sensors and information received from leader and other AGVs state through communication (WiFi)

AGV local speed sensor emits wrong value, encoder feedback unable to be transferred, location sensor estimates the incorrect location and direction  

Speed sensor failure, wheel encoder failure, position encoder failure  

Using only local (speed and location) sensors lead to lateral and longitudinal instability, increasing oscillations, and unsafe behaviour of the platoon; machine damage; major environmental damage; human injuries or life loss  

Take the relative speed and distances of front and rear AGVs as well as absolute location and tracking speed information from leader AGV through communication. Based on these variables the correct desired speed will be re-evaluated. AGV will use the sensor fusion to make estimations of missing data

Difficult to localize and detect obstacle, cannot take the whole picture of object, sends a wrong message to internal part of the system  

Improper lighting; blind spot; object is too far or too close; dirty or damaged lens; position encoder failure  

Increase oscillations and unsafe behaviour of the platoon; collision with other obstacles may happen; machine damage; human injuries or life loss  

Chauffeur will take the decisions based on leader and front AGVs information that are received through V2V communication link, motion manager and ego wheel speed sensor

AGV black out and stop functioning due to sudden power or electrical system failure  

Short circuit inside AGV  

The collision of AGV with other AGVs in platooning may happen; machine damage; loss of critical hardware; major environmental damage  

The rear AGV will take the decision based on its on-board sensors; to manage tracking distance apply the brake to slow down the speed or stop. The fog controller gives the command to leader, which forwards the commands to faulty AGV to leave the platoon, or otherwise rear AGV to rotate the steering wheel and/or change the lane

Table 1: Extract of the HAZOP Analysis Report for AGV Platoon Safety

<table>
<thead>
<tr>
<th>Item</th>
<th>Guide words</th>
<th>Parameter/Function</th>
<th>Deviation</th>
<th>Cause</th>
<th>Consequence/ Effect</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>H_S1</td>
<td>Not, Failure</td>
<td>Brake system</td>
<td>Degradation of braking system performance, fails to deliver the requested torque</td>
<td>Broken motor, loss of power, fluid leakage</td>
<td>The collision of AGV with other machines or human worker may happen; loss of critical hardware and human injuries or life loss</td>
<td>AGV should use auxiliary brake system sufficiently at early/right time and send status information to leader and rear AGVs; the rear AGVs will take decision based on its on-board sensors and information received from leader and other AGVs state through communication (WiFi)</td>
</tr>
<tr>
<td>H_S2</td>
<td>Incorrect, Other than</td>
<td>Wheel speed sensor and location sensor (GPS)</td>
<td>AGV local speed sensor emits wrong value, encoder feedback unable to be transferred, location sensor estimates the incorrect location and direction</td>
<td>Speed sensor failure, wheel encoder failure, position encoder failure</td>
<td>Using only local (speed and location) sensors lead to lateral and longitudinal instability, increasing oscillations, and unsafe behaviour of the platoon; machine damage; major environmental damage; human injuries or life loss</td>
<td>Take the relative speed and distances of front and rear AGVs as well as absolute location and tracking speed information from leader AGV through communication. Based on these variables the correct desired speed will be re-evaluated. AGV will use the sensor fusion to make estimations of missing data</td>
</tr>
<tr>
<td>H_S3</td>
<td>No, Part of</td>
<td>Obstacle detection device (Camera, LiDAR)</td>
<td>Difficult to localize and detect obstacle, cannot take the whole picture of object, sends a wrong message to internal part of the system</td>
<td>Improper lighting; blind spot; object is too far or too close; dirty or damaged lens; position encoder failure</td>
<td>Increase oscillations and unsafe behaviour of the platoon; collision with other obstacles may happen; machine damage; human injuries or life loss</td>
<td>Chauffeur will take the decisions based on leader and front AGVs information that are received through V2V communication link, motion manager and ego wheel speed sensor</td>
</tr>
<tr>
<td>H_S4</td>
<td>Not, Failure</td>
<td>Power, electrical system</td>
<td>AGV black out and stop functioning due to sudden power or electrical system failure</td>
<td>Short circuit inside AGV</td>
<td>The collision of AGV with other AGVs in platooning may happen; machine damage; loss of critical hardware; major environmental damage</td>
<td>The rear AGV will take the decision based on its on-board sensors; to manage tracking distance apply the brake to slow down the speed or stop. The fog controller gives the command to leader, which forwards the commands to faulty AGV to leave the platoon, or otherwise rear AGV to rotate the steering wheel and/or change the lane</td>
</tr>
</tbody>
</table>

The safety and security goals related to the prevention or mitigation of the hazards and threats are derived from the analyses results, in order to avoid unacceptable risks. The main goal “the collisions of AGVs that operate in a platoon are avoided...”

The eavesdropping and tampering attacks/threats (see T_S2 item) can read, tamper or override the AGV sensors data, alter electronic control units (ECUs) message and disrupt the vehicle automation system through communication data, which in turn leads to unintended movement of an AGV, for example, enforce AGV to travel at very low speed, initiate strong braking or control steering. The encryption-decryption mechanism could be used to improve security of exchange messages. Another countermeasure for eavesdropping and tampering is to apply anomaly-based detection method that would delete the anomalies in message if an AGV is compromised. In case of replay an attacker saved the information that is previously transmitted by an AGV (see T_S3 item). Afterwards, it re-transmits the outdated messages, such as incorrect speed and previous location in the platoon, whereas in delay and suppression attacker holds information (e.g., warning message about obstacle, change lane) and deliver it late, thereby leading to mission failure or collision. In addition to the message authentication scheme, monitoring, time-delay variation could be checked to prevent such attacks. The Denial of Service (DoS) attack (see T_S4 item) prevents AGVs from receiving or processing information coming from legitimate members and keeps network busy/jam by injecting false and unauthorised messages. Consequently, delay in communication or packet loss can affect the platoon safety and efficiency significantly. The similarity metrics can be used to detect DoS attacks, which would compare the number of messages sent and resource availability. If deviation is detected, the method will delete the unnecessary message, estimate the size of delay and re-transmit the message.
in a production site satisfied to SIL 3", is formulated as shown in Figure 5. This goal does not point out any particular failure in one AGV but rather in the platoon itself. The Safety Integrity Level (SIL) attribute of a safety (or safety-relevant security) requirement indicates the requested level of confidence that an unwanted event will not happen, i.e., violation of that safety or security requirement. Since multiple AGVs are involved in platoon rather than single one, the hazardous events severity is significantly higher. Therefore, the required SIL of cooperative systems, such as AGV platooning is high and requires more attention. To achieve the main goal, several safety and security requirements are derived by considering the collaborative perspective of an AGV, such as “the AGV provides the required properties for managing the tracking distance with front and rear AGVs” and “unauthorised individual shall not tamper or override the AGV data, which can lead to unintended acceleration, braking, steering and obstacle collision”. After identifying the requirements, assume-guarantee contracts are documented for incorrect or unexpected behaviour. The assurance case is constructed for the materials transportation with AGV platooning and contracts are associated with them for unexpected behaviour. Some goals are created as undeveloped claims that require further development. The evidence for undeveloped claims is obtained by simulation. For instance, the evidence obtained from the platooning simulation for adapting new travel direction, locating obstacles in range and collision avoidance is attached to the assurance case.

### 3.3. Verification and Validation with Digital Twin

The concept of digital twin is to use a digital representation of the real-world systems. Specifically, the functions, behaviour, and communication capabilities are mirrored in the digital twin.
to perform system verification and validation. The measures for mishap prevention or mitigation translated into the safety and security requirements are incorporated in the production site scenario as code scripts. However, the systems with enhanced automation, digitalization and connectivity may involve some risks that can just be identified when a mishap occurs, but if the probability is small, the risks may not be detected, so they never happens. To perform the verification and validation of platooning strategy, the simulators of real Volvo Construction Equipment (VCE) machines fabricated by Oryx\textsuperscript{1} are used. The Volvo CE mobile platforms used for training the operators of articulated haulers, excavators, and wheel loaders are connected to the quarry site to demonstrate the functionality and behaviour of manually-driven machines. This means that the connected human-driven machines can operate in conjunction with the other machines in the quarry site. For instance, the rocks transportation in the quarry site can be carried out with the human-driven (articulated) and/or autonomous haulers. In the production site, besides the different machines, the locations/zones are marked in the map and paths are defined between them. The autonomous haulers/AGVs used for materials transportation in site travel in the predefined paths.

The digital twin served as a resource to discover additional hazards and threats, as well as to gain confidence. The AGVs collided in congested zones even with the presence of collision avoidance system. In this case, the geofences are particularly useful by enforcing a zero-speed limit at the entry of the congested zone. The operation of AGVs and manually-driven machines in conjunction also lead to collisions and is currently regarded as unsafe. Accordingly, the humans and manually-driven machines need to get permission to enter autonomous operation zone. The additional uphill and downhill hazards that may lead to positioning errors, clockwise rotation and collisions are determined. For the security reasons, the emphasis is placed on sharing minimal information with other machines. In case of a DoS attack on the V2V communication link, the speed and position values from front AGV are no longer provided to a rear AGV. To eliminate or otherwise mitigate mishap risk, the platoon is broken and rear AGV switched to its on-board sensors.

3.4. Ensuring Operational Safety and Security

The incorrect or unexpected behaviour including the unintended acceleration, brake or steering, which can be caused due to the propagation of malicious message or actuation performance are prevented and mitigated. However, the AGVs in a platoon may encounter new risks during operation that are not considered during design and development phase. The autonomous vehicles underlie the need for managing operational risks in a dynamic manner [20]. Accordingly, the operational data is gathered from simulators to continuously monitor the platoon operations. It is checked whether the conditions made on the environment guarantees the certain behaviour. If the deviations between the expected and correct behaviour are identified, such as sensors and actuators performance, then instead of a single AGV, the behaviour is also checked for others, to evaluate the potential implications and determine the corresponding control actions. The encryption-decryption scheme, message authentication and monitoring (delay variations checks) are used for secure message exchange. The injected attacks related to the tampering, replaying, message falsification and DoS are prevented or mitigated. In another work, we focused on blockchain and smart contracts for secure data exchange between drone and haulers/AGVs [14]. The update of assurance cases is carried out based on the risk control actions. Besides the safety, the required changes in security and associated contracts are tracked and then the update command is launched, so that the gaps in expected behaviour are resolved and current system safety and security is reflected in the assurance cases.

4. Case Study

4.1. Description of the Quarry Site

This section describes an operational quarry site\textsuperscript{2}, which solely produces stone and/or gravel in various dimensions. The quarry operation is carried out using different kinds of machines, for instance, excavator, mobile primary crusher, wheel loader, stationary secondary crusher and haulers. These machines collaborate together to realize the targeted production goals that can be seen as a system of systems (SoS). The quarry site is subdivided into the different production zones:

- Feeding Primary Crusher: The excavator feeds the blasted rocks to primary crusher. The primary crusher breaks the blasted rocks into smaller rocks. This is done to facilitate the transportation of rocks to the secondary crusher.
- Direct Loading or Truck Loading: For the discharging purpose, the conveyor belt is attached to the primary crusher. It is therefore possible to directly load the haulers from primary crusher. If primary crusher starts to build a stone pile, the direct loading is disabled. In such case, the hauler will be loaded with a wheel loader from the stone pile (i.e. indirect/truck loading).
- Transportation: Autonomous haulers and/or human-driven articulated haulers are used to transport material in the quarry site. The operation of autonomous haulers is similar to the AGVs. For the perception of surrounding environment, two obstacle detection sensors, in particular, a LiDAR and a camera are mounted whereas the GPS is fitted for tracking and navigation purposes. The data produced by the particular sensors is processed for controlling the mechanical parts, for example, the drive unit, steering system, and the braking/throttling system [12].
- Dumping and Feeding Secondary Crusher: The autonomous haulers move in the defined paths and dump the loaded rocks in the feeding spot of the secondary

\textsuperscript{1}https://www.oryx.se/

crusher. The secondary crusher further crushes the rocks into smaller granularity or fractions to meet the customer demands.

- Charging: There are designated charging stations to recharge the battery whenever needed. If the energy consumption of the autonomous hauler is reduced, then battery needs to be less often charged. Energy consumption also depends on distance between different zones.

- Parking: The machines are moved to the parking zone after the termination of transportation operation and for maintenance purposes. For the assignment of specific places, the number and kind of machines needs to be determined.

4.2. Digital Twin of Quarry Site

For designing and configuring the quarry site, we have extended and adapted the Volvo CE simulators, fabricated by Oryx\(^3\). They serve as digital twins of various machines used at the quarry site, such as the autonomous haulers/AGVs, the mobile primary crusher, the secondary crusher, the excavator, and the wheel loader. The specific spots/zones are marked in the site map, e.g., loading and dumping. The transportation paths are also defined that operating machines use to move between different zones. In the quarry site scenario, we used autonomous haulers/AGVs for materials transportation. They travel in the predefined travel paths as a platoon, as shown in Figure 4. Three autonomous haulers arrived at the loading zone and make a queue for loading materials as shown in Figure 4a. After loading two autonomous haulers are moving at a slow speed and waiting for the third to complete the platoon (see Figure 4b). After that a platoon moves towards unloading/dumping zone (see Figure 4c). When a platoon moves in a curved path the distance between autonomous haulers are increased (see Figure 4d), however, the gaps are covered after curved path ends, and they are travelling in a straight line (see Figure 4e). When the platoon are approaching to the dumping zone (see Figure 4f). The autonomous haulers split from the platoon for dumping the loaded material (see Figure 4g and h). After completion of unloading, autonomous hauler start moving towards loading area (see Figure 4i).

The autonomous haulers/AGVs are equipped by a chauffeur with a collision avoidance capability. The parameter including current, tracking and desired speeds, desired steering, look-ahead, look back, minimum distance, tracking distance and absolute location are defined. Their values are retrieved and changed during operation. Look-ahead is used to exploit information about known future disturbances acting on the autonomous haulers, such as predicted behaviour of front autonomous haulers that help in avoiding unnecessary braking during downhills. If the speed of a front autonomous hauler/AGV was reduced then the speed of rear au-

\(^3\)https://www.oryx.se/
The collisions of AGVs that operate in a platoon are avoided in a production site satisfied to SIL 3.
tonomous hauler is matched with the front autonomous hauler to manage 10m tracking distance. If the distance between two haulers/AGVs is less than the minimum distance, then the rear autonomous hauler adjusts its speed. However, a look-back is specified to get the information of rear autonomous hauler, for instance, if the brake of a rear autonomous hauler is failed and tracking distance is less than 10m, then front autonomous hauler will increase the speed to manage safe tracking distance.

4.3 Dynamic Risk Management

The distance between autonomous haulers/AGVs is increased in the curves. A human-driven hauler is added in the platoon. To manage risk of an added human-driven hauler, the platoon is broken and the corresponding autonomous hauler is made a leader. In circumstances the primary crusher is jammed, the fog controller is notified that gives command to the platoon leader to approach the dumping zone without waiting for other autonomous haulers. The deviations in behaviour may lead to partial or full non-conformance. If the deviations in sensors and actuators performance, such as speed, steering, braking or visibility are encountered, instead of a single AGV, the behaviour of others is checked, to determine the corresponding control measures. In case of a slippery surface, all the AGVs may encounter an increased braking distance. As a preventive measure, their safe tracking distances are increased based on the determined threshold. When the problem in maintaining path position and steering are encountered, the threshold is covered by reducing the speed limit.

The current speed is an essential factor for calculating desired steering. To adapt a new direction, the current and desired speed, desired steering as well as acceleration range are considered. In addition to the measures for whole site, the problems at specific path points, time frames, and their corresponding measures are recorded. To understand the impact of impersonation, falsification and tampering attacks in autonomous haulers/AGVs platoon performance, we injected the erroneous messages. In particular, we tampered the parameter values of an autonomous hauler i.e. increased and decreased its current speed, and alter its current position. For replay, DoS, and suppression attacks, we recorded the acceleration value of an ego autonomous hauler, and sent this value again to itself and rear autonomous hauler. These attacks are detected and corrected by our platooning strategy. The update of assurance cases is carried out based on the selected risk control actions. The contracts derived for uncertainty sources are associated with the assurance case elements. They are monitored by comparing with the operational data gathered from the simulations. To resolve the gaps with the contracts, i.e., the assumptions made and guarantees provided, the confidence, in certain situations, such as operating speed and tracking distance are gradually fine tuned. In this way, the simulation result related to the satisfied contracts is assembled as an evidence to the undeveloped claims, such as “propsNewDir” and “propsCollAvoid”, as shown in Figure 5. When the deviations or mismatches are detected, the affected parts of assurance cases are tracked and adapted to reflect the current safety and security of AGV platooning. The interested reader may refer to our previous work [1] for further details of update of contracts and assurance cases.

5. Related Work

The automated vehicles/AGVs are vital for materials transportation in advanced production sites and Industry 4.0 contexts. In our previous research, the materials transportation in production sites and Industry 4.0 is targeted. The performed analysis for Industry 4.0 not just focuses on the individual behaviour of AGV, but also the emergent interactions of AGVs, with fog/cloud server or other working equipment [1, 13]. To support the dynamic reconfiguration, the hazard analysis is performed by explicitly considering the modularity, scalability, diagnoseability, customizability, convertibility and integrability characteristics. The geofences are used as an active countermeasure for dynamic risks management in automated transportation/production contexts [20]. In these works, the safety assurance process is followed during design and development, then the verification and validation is performed with simulation-based digital twins, and finally dynamic risk management is conducted during operational phase. This paper, however, focuses on the safe and secure AGV platooning for materials transportation. Accordingly, the safety and security analysis is performed to identify potential platooning hazards, threats, vulnerabilities, their potential effects and the reliability of AGV platooning in Industry 4.0. The published studies have not considered the platooning for materials transportation in production sites and Industry 4.0.

Petrillo et al. [21] present a consensus-based control strategy (i.e. voting procedure) to tackle the platoon control problem in the presence of message falsification attacks. Each vehicle is checked to detect anomalies in the wirelessly received data from the members group with a collaborative decision making technique. Biron et al. [22] propose a framework based on adaptive estimation and sliding mode theory that can detect the occurrence of a denial of service attack, which is modeled as unknown constant delay and estimate the effect of the attack on the connected vehicle system. He et al. [23] introduce a method to detect potentially attacked GPS data in an unknown vehicle, which consists of a local state observer (a saturation-like scheme), two online attack detectors and a distributed controller. Zhu et al. [24] study the security issues and use the platooning case study to show their harmfulness. The work presented in this paper focuses on the simulation of AGV platooning in production sites, dynamic risk management during operational phase and update of assurance cases constructed for platoon.

A systematic literature review carried out on safety in vehicles platooning reveals a dearth of comprehensive research on different aspects of platoon including safety analysis [4]. Nilsson et al. [5] investigated the cooperative platooning perspective with ISO 26262 using a platooning scenario. The issues arise because of the hazard analysis and risk assessment (HA&RA) and functional safety concept. To cope with them, all the vehicles which are part of the cooperative functionality are included in the safety lifecycle. To accommodate the hazardous
events in cooperative systems with highest risk factor, they introduced a new severity class (S4) and consequently ASIL E. Mizuma and Nakamura [6] perform the safety evaluation of bus transportation system. They use IEC 61508 together with FTA. Slijivo et al. [7] presents a contract-based methodology for assurance of design patterns. They used PolarSys CHESS and PolarSys OpenCert tools to specify the design and assurance case patterns, respectively. The cruise control and car platooning modes are used for exemplification. In this paper, the safety and security analyses for AGV platooning in production site are performed by using the HAZOP and THROP techniques, respectively. In addition to the construction of assurance cases, their update during operational phase is performed to reflect the observed safety and security of AGV platoons.

6. Conclusion and Future Work

This paper targets the safe and secure platooning of AGVs in Industry 4.0 scenarios. The hazard and threat analyses techniques, particularly HAZOP and THROP, are applied to identify hazards, threats, vulnerabilities, their potential effects and the reliability of AGV platooning in Industry 4.0. The safety and security requirements are derived based on the analyses results to prevent/mitigate the potential hazards and attacks. We utilise simulation-based digital twins to perform verification and validation. In particular, the platooning strategy is implemented in the Volvo CE digital twin fabricated by Oryx. The AGV platoon detects and avoids risks, such as speed limits, subsystem failures, and prevents unauthorised access, spoofing, tampering and denial of service attacks, etc. As the platooning in Industry 4.0 underlie the need for dynamic risk management, operational data is used for identifying, monitoring, evaluating and resolving mishap risks. To avoid the culture of just reflecting the intended system behaviour, the assurance (safety and security) cases are updated with respect to the observed system behaviour. The AGV platooning not just improve safety, security and efficiency, but also reduce resource usage. The applicability has been demonstrated for the transportation in a quarry site that is transformed to comply with Industry 4.0.

The work presented in this paper is generally applicable to both outdoor and indoor sites based on the Industry 4.0. In the quarry site, the autonomous and human-driven machines can be used for materials transportation. If a human-driven machine is permitted to operate in conjunction with AGVs, then it could be used as a platoon leader. The threats to validity includes the large loading time, short range materials transportation and arbitrary traffic flow to different locations. In the future, we intend to control the AGV platoon by using a drone. Another direction for future work is to adapt and extend the autonomous driving simulators, such as AirmSim and Carla for platooning on public roads. In this regard, the additional hazards and threats, regulations, such as traffic rules and ethical aspects will be considered.

Acknowledgment

This work is supported by InSecTT (Intelligent Secure TrustableThings), ESCAPE (Efficient and effective functional safety for complex autonomous production systems) and FiC (Future factories in the Cloud) projects. InSecTT has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 876038. The JU receives support from the European Union’s Horizon 2020 research and innovation programme and Austria, Sweden, Spain, Italy, France, Portugal, Ireland, Finland, Slovenia, Poland, Netherlands, Turkey. ESCAPE project has received funding from the FiA (Process industrial IT and Automation) program which is financed through Vinnova, while the FiC project is funded by the SSF (Swedish Foundation for Strategic Research). The first author has also participated during the tenure of an ERCIM “Alain Bensousan” Fellowship Programme.

References


Muhammad Atif Javed is currently an ERCIM fellow and a visiting researcher at RISE SICS Västerås, Sweden. Before that, he was a researcher at Mälardalen University, Sweden. His research interests include autonomous robots/vehicles, safety and security assurance, reconfigurable systems, digital twins, and Industry 4.0. He received his Dr. tech. degree from the University of Vienna, Austria in 2016.

Faiz Ul Muram is a biträdande lektor at Linnaeus University, Sweden. Before that, she worked as a researcher at Mälardalen University, Sweden. Her research focuses on process engineering, compliance management, behaviour models, system-of-systems, safety and security assurance, formal verification, IoT, digital twins and model-driven engineering. She received her Dr. tech. degree from the University of Vienna, Austria in 2017.

Sasikumar Punnekkat is a professor in dependable software engineering at Mälardalen University and the leader of the Dependable Software Engineering research group. His research focuses on dependable real-time systems, fault-tolerant computing, software engineering, functional safety, software reliability, and software testing. He was awarded Doctor of Philosophy in Computer Science by the University of York, UK in 1997.

Hans Hansson is professor in Real-Time Systems at Mälardalen University since 1997. He is director of Mälardalen Real-Time Research Centre, Scientific Leader at RISE SICS Västerås. His research focus on distributed embedded systems with contributions in data communication, real-time systems, system development, and modelling & analysis. He received a Doctor of Technology degree (Computer Systems) from Uppsala University, Sweden, in 1992.