Safety analysis on typical scenarios of GTCS based on STAMP and STPA

Yuwen Qi¹, Yuan Cao²³*, Yongkui Sun³

¹ CRRC Changchun Railway Vehicles Co. Ltd., 130062 Changchun, Jilin, China
² National Engineering Research Center of Rail Transportation Operation Control System, Beijing Jiaotong University, 100044 Beijing, China
³ School of Electronic and Information Engineering, Beijing Jiaotong University, 100044 Beijing, China

*Corresponding author e-mail: ycao@bjtu.edu.cn

Abstract. As the rapid development of the urbanization, solutions to solving the traffic congestion have become a hotspot. In this case, the Guided Transportation System (GTS) has been developed, which has the potential to release the traffic jam due to the advantages of short construction period and low cost. Safety analysis on the new transportation tool is essential to keep its operation and passengers safe. Based on the STAMP (Systems-theoretic Accident Modeling and Processes) model and the STPA method (System-theory Process Analysis), this paper constructs a safety analysis framework for the typical operating scenarios of the Guided Transportation Control System (GTCS). Aimed at typical scenarios of vehicle tracking, the corresponding hierarchical control structure models are established. Then, the hazard causes are analyzed. And corresponding safety constraints are put forward to handle the hazard causes, which can provide supports for improving the system design of the GTCS.

1. Introduction

Nowadays, the city size and population in China have continued to expand, which results in heavy traffic congestion. Most urban planning funds in second- and third-tier cities are invested in the real estate industry, which means that for these cities, they do not have more funds to afford the high construction costs of rail transit. Therefore, the selection of traditional public transportation is the root cause of traffic congestion.

In recent years, China’s independent science and technology develop rapidly. In this case, taking the advantages of tram and bus, the GTS vehicle [1-3] has been developed as a new modern transportation tool to release the traffic congestion. Different from the existing rail transit, such as metro, tram, the GTS vehicle runs on virtual track instead of physical track. The virtual track is realized using track marking line, which can be easily sprayed on the ground. So the construction period can be greatly shortened, and the construction costs can be greatly reduced. In addition, as the GTS vehicle uses electricity to supply energy, it will not pollute the environment.

With the continuous improvement and development of automation technology, the technology of using the train control operation system to realize driverless train has become a hotspot [4-6]. While the GTS vehicle has great potential to realize driverless operation, which can save lots of human resources. As a new transportation vehicle, the GTS vehicle is also controlled by a set of control system. However, if a system is to be put into use, the most basic thing is undoubtedly to ensure that the
system can operate safely. Therefore, the safety analysis becomes the focus for analyzing the safety of the system. However, with the complexity of vehicle functions, safety analysis of systems has become a huge challenge.

Safety is the most important topic in the field of transportation. The goal of safety analysis is to identify causes of the potential accidents, to eliminate or control them during the design stage or before operation. Traditional risk analysis methods treat hazards as the result of a series of events that often involve multiple types of component failures or human error. There have been some safety analysis methods, such as failure mode and effects analysis (FMEA) \[7\] and fault tree analysis (FTA) \[8\]. These methods are suitable for analyzing losses caused by physical component failures and relatively simple systems. However, the GTCS is complex, which includes lots of functions. The above mentioned analysis methods are not suitable for the GTCS, because the analysis process will become very complex. The system-theoretic accident modeling and processes (STAMP) model was first proposed by Leveson in 2004, and has been continuously explored, improved and developed by experts and scholars in various fields \[9\]. Now, it has been widely used in the analysis and research of safety issues in various fields, such as aerospace industry \[10\], railway industry \[11\] and missile \[12\].

Unlike traditional system safety analysis methods, STAMP treats the system as an entirety when analyzing system safety, and treats safety as a problem caused by unsafe controlling \[13\]. The STAMP safety idea is that accident prevention requires identification and elimination (or mitigation) of unsafe interactions among components, such as strengthening control and strengthening relative safety constraints during system development, design, and operation. There have been cases in which the STAMP model is used to analyze the CTCS (China Train Control System)-3 level \[14\] and the CBTC (Communication Based Train Control System) \[15\] in detail. However, the GTS vehicle is much different from the traditional rail train, which runs on the street and does not rely on physical rails. The road conditions in the city are extremely complicated. Except system itself, pedestrians and vehicles can also cause dangers and even result in heavy accidents. So compared with the train control system of the traditional rail train, the hazard sources of the GTCS become more complex. Accordingly, the constraint conditions also change greatly. For rail train control systems, such as CBTC, brake should be taken immediately to ensure safety when the speed of the train exceeds the safety protection curve. The constraint condition is that brake measure is taken when the train overspeeds. For the GTS vehicle, it is not only the case. It is necessary to take the safety of pedestrians on the road into account while protecting the safety of the vehicle. So, it is essential to make safety analysis on the GTCS. As a set of top-down safety analysis models, STAMP is suitable for analyzing the safety of complex dynamic systems.

2. Safety analysis method for the GTCS based on STAMP and STPA

2.1. STAMP Theory

The STAMP model is based on system theory and treats system safety as the emergence property of a complex system. Safety accidents are caused by unsafe interactions of components during operation due to unsafe control actions in design, development, and operation, which is a dynamic process with a slow transition from a safe state to a high-risk state. The STAMP uses a multi-level control structure modeling approach to build the safety control structure model. The control structure is used to describe responsibilities and permissions among system components. The upper layer of the control structure is a controller with a process model. The process model generates control commands through the transition of the controlled state and the calculation of the control algorithm to control the lower controlled objects through the actuator to complete target activities. The lower-level controlled objects are monitored by feedback devices while executing the upper-level instructions. The feedback device feeds the information back to the upper-level controller in real time. The controller refers to the safety model and corrects the internal state of the model according to the feedback information. An accident may occur when the internal state and feedback of the process model are inconsistent. The STAMP method analyzes the possible risks in the control structure, and determines safety constraints to eliminate or control them.
2.2. STPA Method

The STPA method is a system safety analysis method based on the STAMP model. By constructing a control and feedback loop consisting of controllers, actuators, control processes and sensors (Fig. 1), the STPA safety analysis method establishes corresponding safety constraints on possible accidents by defining system-level accidents and building system control process models. When analyzing the safety risks through the system control process model, it is necessary to analyze safety requirements and all control actions in each part to identify the potentially dangerous control actions to improve the safety constraints of the system.

![Control and feedback loop diagram]

Assume that the system dangerous set is $H = \{H_1, H_2, ..., H_n\}$, the state where no danger is generated is $NoH$, and the $NA$ if not applicable, and a control action is $\Sigma a$, System safety can be expressed as\cite{[16]}:

1. Basic design flaws in the system:

   \[
   (\sum a_{T} \rightarrow H_1) \land (\sum a_{TN} \rightarrow H_1) \tag{1}
   \]

2. Design conflict between two security requirements of the system:

   \[
   (\sum a_{T} \rightarrow H_1) \land (\sum a_{TN} \rightarrow H_1) \tag{2}
   \]

3. If the control action is dangerous, but the control action is not dangerous, then the requirement of the system in the environment $E$, the control action is not provided:

   \[
   (\sum a_{T} \rightarrow H_1) \land (\sum a_{TN} \rightarrow NoH), and R = \sum a_{TN} \tag{3}
   \]

4. If providing control action does not cause danger, but not providing control action creates danger, then the requirement of the system at this time is under environment $E$, and control action should be provided:

   \[
   (\sum a_{T} \rightarrow NoH) \land (\sum a_{TN} \rightarrow H_1), and R = \sum a_{T} \tag{4}
   \]

5. If the provision of control actions does not cause danger, the provision of control actions prematurely or too late creates danger, which lasts too long or ends too quickly. Not applicable, but the provision of control actions does not cause danger. At this time, the system needs to provide control actions (at this time It can be analyzed that the control action is discrete), and the control action has strict timeliness, and the demand for discrete control actions with strict timeliness is represented here by $RDT$:

   \[
   (\sum a_{T} \rightarrow NoH) \land (\sum a_{TN} \rightarrow H_1) \land (\sum a_{TOLP} \rightarrow H_1) \land (\sum a_{TOSLP} \rightarrow NA), and R^{DT} = \sum a_{T} \tag{5}
   \]

6. If there is no danger in providing the control action, it is dangerous to provide the control action too early or too late and continue too long or end too quickly, but if the control action is not provided to cause danger, then the system needs to provide the control action (control action It is continuous type), and the control action has strict timeliness. The demand for continuous control action with strict timeliness is represented by $RCT$ here:

   \[
   (\sum a_{T} \rightarrow NoH) \land (\sum a_{TN} \rightarrow H_1) \land (\sum a_{TOLP} \rightarrow H_1) \lor (\sum a_{TOSLP} \rightarrow NoH) \land (\sum a_{TLOSP} \rightarrow H_1), and R^{CT} = \sum a_{T} \tag{6}
   \]
In the above expression, $A$ is the controlling party, $B$ is the controlled object, $E$ is the environment, $P$ is "Providing" creates danger, $NP$ is "Not providing" creates danger, $EoLP$ is "Providing too early or too late" creates danger, $LoSP$ is "It lasts too long or ends too quickly" creates danger.

2.3. Safety Analysis Method for the GTCS

Based on the STAMP theory, STPA method and safety requirements, this paper proposed a safety analysis method to analyze system safety in several typical operating scenarios of the GTS vehicle. By constructing the system hierarchical control structure diagram to identify the hazard sources to eliminate unsafe control actions and reduce system risks. The framework of the proposed safety analysis method is shown in Fig. 2.

![Figure 2. The framework of the proposed safety analysis method.](image)

3. Safety analysis of the GTCS

3.1. Hierarchical Control Structure Establishment

The wheel structure of the GTS vehicle is the same as that of the bus. The wheels are controlled by an independent steering system. This means that there may be deviations from the virtual orbit during the tracking of the GTS vehicle. In normal operation, the deviations can be controlled in an acceptable range by GTCS. In some cases, the vehicle needs to actively deviate from the track. For example, when an obstacle suddenly catches the road, the GTS vehicle can immediately make an avoidance action at the same time as the emergency braking, thereby reducing the damage of itself and the obstacles. Therefore, in the tracking process, safety analysis is an important step when there are obstacles on the road.

Through the analysis of GTCS, the hierarchical control structure diagram in the typical scene of vehicle tracking is given as Fig. 3.

![Figure 3. Hierarchical control structure diagram of vehicle tracking.](image)

In the process of vehicle tracking, the on-board control system is used as the main controller. It needs to refer to the safety model to calculate the control commands in real time according to the feedback information of the sensors. The speed control controller and direction control controller receive the commands and carry out corresponding actions to keep vehicle operating safely. In the case of obstacles, the on-board control system needs to control the direction control controller to turn in time according to the position of the obstacle. At the same time, the speed control controller performs emergency braking to ensure the safety of the vehicle and obstacles. In the tracking scenario, the main control actions of the on-board control system include:
(1) In normal operation, the speed control subsystem of the on-board control system ensures the vehicle runs at a safe speed.
(2) In normal operation, the direction control subsystem of the on-board control system ensures the vehicle runs on the track.
(3) When the obstacles occur on the road, the speed control subsystem makes the vehicle brake urgently to make the speed drop to zero.
(4) When the obstacles occur on the road, the direction control subsystem makes the vehicle urgently avoid the obstacles.

3.2. Unsafe Control Actions (UCAs).
According to the hierarchical control structure diagram, the safety requirements, and the control relationship between each level can be seen intuitively. The UCAs that may occur during the tracking of the GTS vehicle is shown in Table 1.

| System-level hazard | Control action | Not be executed | Incorrect execution | Control is carried out too early or too late | Execution time of this control is too short or too long |
|---------------------|----------------|-----------------|---------------------|--------------------------------------|---------------------------------------------|
| H1. Vehicle speed is out of control | Emergency brake | UCA1: When an obstacle hits the road, the on-board control system does not send the emergency braking command, causing the vehicle hits the obstacle. | UCA4: When an obstacle hits the road, the on-board control system does not send an emergency braking command in time, causing the vehicle hits the obstacle. | UCA6: When an obstacle hits the road, the brake command sent by the on-board control system ends too fast, causing the speed does not drop to zero. |
| H2. Vehicle direction is out of control | On-board system control vehicle direction | UCA2: When an obstacle hits the road, the on-board control system does not send the emergency avoidance command, causing the vehicle hits the obstacle. | UCA3: When an obstacle hits the road, the on-board control system sends the wrong steering command, causing the vehicle fails to avoid the obstacle or collide with other vehicles. | UCA5: When an obstacle hits the road, the on-board control system does not send an emergency avoidance command in time, causing the vehicle hits the obstacle. |

3.3. Causes Analysis and Safety Constrains.
The ATC (Automatic Train Control) system in the on-board equipment is the main controller, which include ATP (Automatic Train Protection) and ATO (Automatic Train Operation). When the obstacle suddenly hits the road, the distance sensor measures the distance between the vehicle and the obstacle. And the data is fed back to the ATP in real time. The ATP calculates and makes a safety judgment. When it is judged to be dangerous, an urgent brake and steering commands are sent to the ATO. The ATO controls the vehicle speed controller and direction controller to brake and turn direction. By analysis, the causes and safety constrains are given in Table 2.
Table 2. Hazard source analysis

| UAC       | causes                                                                 | Safety constrains                                      |
|-----------|------------------------------------------------------------------------|--------------------------------------------------------|
| UCA1, UCA2| The sensor fails or the interface between the sensor and on-board equipment is abnormal. ATP does not receive feedback information from the sensor. | If the ATP cannot receive the feedback information from the sensor, the maximum service braking is executed immediately, and the cause of the brake is fed back to the driver via the vehicle. The on-board equipment needs to monitor the sensor status and the interface status between the sensor and the on-board equipment in real time. Once abnormal case is detected, it needs to be immediately reported to the driver. |
| ATP does not effectively output emergency braking or emergency avoidance commands. | Daily inspection is required before the vehicle operations to ensure that the vehicles’ performance and components are normal. ATP needs to cut off the vehicle traction after outputting the emergency braking command until the emergency braking is turned off. |
| ATP uses the wrong database, causing error output. | Line data should be downloaded before the vehicle is put into daily operation. The vehicle on-board equipment should have the function of updating data during normal operation, and update the database regularly. |
| Vehicle runaway |                                                                                 | Vehicle traction must be removed after the vehicle speed drops to zero. If the vehicle runaway is detected and the distance or speed exceeds the tolerance range, then the ATC needs to implement braking to ensure safety. |
| The vehicle that ATO self-inspection fails was put into operation, causing the vehicle braking fails. | ATO self-inspection should be carried out. If not meet the requirements, the feedback information should be uploaded in time. |
| Speed or position error is too large |                                                                                 | Speed sensors must feedback vehicle speed information in real time to reduce speed measurement errors. The on-board equipment should be able to identify the wheel slipping state, and the ATP needs to correct the vehicle speed. Ensure that the vehicle wheel diameter in the database is accurate and update the information as soon as the vehicle changes wheels. |
| UCA3 | The sensor does not feedback the obstacle position information, causing the ATP fails to confirm the steering direction. | The sensor should feedback the obstacle position information in time. If the sensor does not feedback the obstacle position information, the driver should perform manual steering to avoid collision. |
| UCA4, UCA5 | It takes ATP too long time to process feedback information and send instructions to ATO | ATP must complete the processing for sensor feedback information and send instructions to ATO within the specified time. If not, the vehicle implements the maximum service braking and displays the notification to the driver. |
| It takes ATO too long time to process the information sent by ATP. | The ATO must complete the processing of the ATP transmission command and feedback results to ATP within the specified time. If not, the driver must be alerted immediately and the driver is prompted to perform an emergency braking. |
| UCA6 | ATP emergency brake command is lifted too early. | When the vehicle speed drops to zero, the emergency brake can be released. |
| During braking, ATP stops the brake due to calculating wrong results based on the old data fed back from the sensor. | Once any information fed back by the sensors is updated, the old information is considered invalid and cannot be used for calculation. |
| ATO cancels the emergency braking too early. | ATO needs to strictly execute the ATP instructions and feedback the current execution status in real time. |
| During the braking process, the interface between the on-board equipment and speed controller is faulty and the braking stops. | If the interface fails, the maximum service braking should be executed immediately, and fault cause should be fed back to the driver. |
4. Conclusion

Based on the STAMP theory and STPA method, this paper carries out the safety analysis of the GTCS. Safety analysis framework of the GTCS is constructed, and the safety analysis flow for the GTCS is summarized. Then, aimed at the typical scenarios of vehicle tracking, UCAs and causes are obtained by analyzing on the established hierarchical control structure diagrams. Some effective measurements are then proposed to handle system-level hazards, which can provide technique supports for the later design and improvement of the GTS vehicle.

5. Acknowledgments

This work was supported by the National Key R&D Program of China (2018 YFB1201601) and China Postdoctoral Science Foundation under Grant (2019M650472).

References

[1] Niu, H.F. Tong, X.W. Lei, Y.F. Li, Z.B. Zhang, X. Peng, J. and Jiang, W.L., Dynamic characteristic test bed and test system development of the electro-hydraulic servo steering system of ART, Chinese Hydraulics & Pneumatics, 2018, vol. 7, p. 120-127.
[2] Zhao, S., Research on key technical scheme of ART signal system, Urban Rail Transit, 2019, vol. 16, no. 5, p. 56-61.
[3] Tan, J.H. Xiao, X.Y. Zhang, H. and Zhang, N., Research on the signal timing method of ART intersection, Computer Era, 2018, vol. 6, pp. 23-25+28.
[4] Wang, Y.H. Zhang, M. Ma, J.Q. and Zhou, X.S., Survey on driverless train operation for urban rail transit systems, Urban Rail Transit, 2016, vol.2, no. 3-4, p.106-113.
[5] Powell, J.P. Fraszczyk, A. Cheong, C.N. and Yeung, H.K., Potential benefits and obstacles of implementing driverless train operation on the tyne and wear metro: a simulation exercise, Urban Rail Transit, 2016, vol. 2, no. 3, p. 1-14.
[6] Tang, M.A. and Wang, P.Q., Automatic train optimization operation based on hybrid system modeling predictive control, Journal of Railway Science and Engineering, 2019, vol. 16, no. 6, p. 1527-1534.
[7] Xu, A.Y.G. Bhatnagar, J. Bednarz, G. Flickinger, J. Arai, Y. Vacsulka, J. Feng, W.Z. Monaco, E. Niranjan, A. and Lusford, L.D., Failure modes and effects analysis (FMEA) for Gamma Knife radiosurgery, Journal of Applied Clinical Medical Physics, 2017, vol. 18, no. 6, p. 152-168.
[8] Kabir, S., An overview of fault tree analysis and its application in model based dependability analysis, Expert Systems with Applications, 2017, vol. 77, p. 114-135.
[9] Leveson, N.G., A systems-theoretic approach to safety in software-intensive systems, IEEE Transactions on Dependable and Secure Computing, 2004, vol. 1, no. 1, p. 66-86.
[10] Kathryn, K.A. Stephanie, C. Mirna, D. Nicolas, D. Nancy, G.L. and David, Z., Engineering spacecraft mission software using a model-based and safety-driven design methodology, Journal of Aerospace Computing Information & Communication, 2015, vol. 3, no. 11, p. 562-586.
[11] Niu, R. Cao, Y. Ge, X.C. and Tang, T., Applying system thinking to learn from accident of modern automatic control systems, Chinese Journal of Electronics, 2014, vol.23, no.2, p.409-414.
[12] Rong, H. and Tian, J., STAMP-Based HRA considering causality within a sociotechnical system: a case of minuteman III missile accident, Human Factors, 2015, vol. 57, no. 3, p. 375-396.
[13] Pawlicki, T. Samost, A. Brown, D.W. Manger, R.P. Kim, G.Y. and Leveson, N.G., Application of systems and control theory-based hazard analysis to radiation oncology, Medical Physics, 2016, vol. 43, no. 3, p. 1514-1530.
[14] Wang, R. and Zheng, W., Research and application of the BFM-STAMP hazard analysis method, Proc. IEEE International Conference on Intelligent Rail Transportation, Beijing, China, 2013, p. 175-179.
[15] Yan, F. Tang, T. and Yan, H.W., Scenario based STPA analysis in automated urban guided transport system, Proc. IEEE International Conference on Intelligent Rail Transportation (ICIRT), Birmingham, UK, 2016, p. 425-431.
[16] Zhou, Y., Research on STPA-Based Safety Analysis of Electronic Checklist of Civil Aircraft, Nanjing University, 2018.