Software/System Safety Case Study – LIDAR and Computer Vision Systems for Autonomous Ground Vehicles

SE575, FA2010
Embry Riddle Aeronautical University, Electrical, Computer, Software & System Engineering

Introduction

This case study describes a safety analysis of the optical components of the navigation system for an autonomous ground vehicle (AGV). Light Detection and Ranging (LIDAR) and a dual-camera computer vision (CV) system were commonly utilized sensor systems for autonomous vehicles, which were the primary components under study.

The research conducted is of increasing importance as fully autonomous vehicles begin to find their way onto roads. Due to the necessity of environmental sensing for these vehicles, LIDAR and CV systems are required, inherently safety-critical, software intensive systems, faults or failures in which could result in mishaps leading to loss of life and property. By analyzing the hazards posed by the system described, the chance of mishap may be reduced or, in some cases, eliminated entirely.

System Description

The system under test is an autonomous ground vehicle (AGV) which combines LIDAR and computer vision systems to form a primary navigation system. Although supplemented in many navigation systems by Inertial Measurement Units (IMUs) or Global Positioning System (GPS) sensors, the accuracy provided by optically-based navigation controls is absolutely necessary for a safe and precise AGV.

LIDAR and CV systems are capable of providing kinematic information about a vehicle’s position, velocity and acceleration. Furthermore, for the AGV hazards classification the probability for something bad or undesired to happen is important to understand that hazards and risks are much related to each other because a risk is a combination of the severity of the consequences of a hazard and the likelihood of occurrence (Korl). Risks specially come into play during the Hazard Classification stage of the Safety Process.

During this stage hazards are classified according to their risks, that is, according to the severity of the consequences and the frequency of occurrence.

After developing the PHA it is now possible to classify these hazards. For the AGV systems we have decided to evaluate the hazards in a qualitative manner, utilizing pre-defined arbitrary categories known as risk classes or risk levels. For the AGV system, these levels are negligible, marginal, critical and catastrophic. Since a risk is variable that results from a composition of frequency and severity of occurrence, it is important to understand that a risk class or level classifies the risk according to the product of the two variables.

A hazard is a situation in which there is potential source for danger or harm to people, property or the environment [SEC-99]. Hazards are a very important component of the entire system safety lifecycle. From a safety standpoint, hazards become the source, or part of the source for the safety requirements of the software intensive system under development.

Typically, the loss of any system functionality will lead to a hazard (i.e. if the laser head of the LIDAR system stops rotating due to mechanical failure). The loss of functionality usually allows us to identify a hazard right away. In turn, the hazard identification step leads to the control elaboration/design step where a control measure is established to prevent or control this hazard. Finally, this control measure can be then converted into a safety requirement for the system under development and thus be taken into consideration in the system’s development lifecycle. Hazards are always dormant, that is, they are existent, but harmless unless certain conditions are achieved. These conditions include the energy build-up, time, a point of no return and degradation of the system safety levels. All these conditions are required in order for a hazard to transform into an accident or mishap.

Analysis

Risk represents the probability for something bad or undesired to happen. It is important to understand that hazards and risks are much related to each other because a risk is a combination of the severity of the consequences of a hazard and the likelihood of occurrence (Korl). Risks specially come into play during the Hazard Classification stage of the Safety Process. During this stage hazards are classified according to their risks, that is, according to the severity of the consequences and the frequency of occurrence.

By utilizing both Fault Tree Analysis (FTA) and BBN it is possible to better determine what are the sequences of events leading to top level mishaps. FTAs are extremely useful tools in safety engineering because they help in identifying the major undesirable event (UE) directly related to a hazard or hazards. Furthermore, the FTA also allows identifying in the process the intermediate events that cause the UE. In this project an FTA was developed for each top level mishap (pedestrian injury, vehicle damage and other damage). These FTAs are shown in Appendix C. Due to the large size of the FTAs, some are divided into smaller diagrams that lead to a major subsystem failure. From the FTA results it is clear that any major mishap will always involve the failure of one or more subsystem components. In the case of both subsystem components failing (cameras and LIDAR) the resulting behavior of the AGV system will always reach a top level mishap scenario.

Lessons Learned

There were many important lessons learned during this project’s development:

- Safety Engineering is a very critical component of any system under development.
- Safety Engineering must be present throughout all the different phases of any product’s lifecycle.
- For Safety Engineering to be carried out successfully it is imperative that the system and its subcomponents are very well understood. Lack of knowledge or understanding will always result in poor safety engineering practices which in turn increase the possibilities for incidents and accidents.
- The hazards identification and classification steps are of critical importance. Failure to identify a hazards will likely lead to an accident when conditions are met. Failure to classify the hazards correctly will likely lead to a bad distribution of time and safety engineering resources.

Conclusions

This project has analyzed an autonomous ground vehicle system's optical navigation components with the goal of reducing or eliminating hazards in a general system. Safety analytical modeling techniques including fault tree analysis and bayesian belief networks were implemented in order to better understand the sequence of events that could lead to a major accident or mishap. These tools also helped in determining the most important hazards and risks that need to be mitigated or controlled in order to reduce the risks for any loss of property or life involving the AGV system. Analysis results confirmed the importance of the reliability and availability of the AGV’s sensor subsystems (LIDAR and Computer Vision). Some of the control measures recommended included careful understanding of system operations manuals for the AGV system and its sub-systems as well as preliminary checklists aimed at inspecting the state of the AGV’s sub-systems and thus preventing hazards from becoming incidents and/or accidents with important consequences.

Bibliography