Safety and Verification for a Mobile Guide Robot

Jonathan M. Aitken, Owen McAree, Luke Boorman, David Cameron, Adriel Chua, Emily C. Collins, Samuel Fernando, James Law, Uriel Martinez-Hernandez
Sheffield Robotics, University of Sheffield

Abstract

This work presents the safety and verification arguments for the development of an autonomous robot platform capable of leading humans around a building. It uses Goal Structuring Notation (GSN) to develop a pattern, a re-usable GSN fragment, that can form part of the safety case surrounding the interaction of a mobile guide robot to: record the decisions taken during the design phase, ensure safe operation around humans, and identify where mitigation must be introduced.

Keywords Goal Structuring Notation; Mobile Robotics; Safety; Verification.

1. Introduction

This paper discusses the safety concerns and formal verification required for deploying an autonomous robot, ROBO-GUIDE [1], which is able to navigate corridors in a building and acquire human help in using a lift to reach different floors. This task will require ROBO-GUIDE to maintain autonomy, while co-existing in an everyday environment, around people not used to robots. This paper discusses hazards that will arise and their safe mitigation.

2. Operational Hazards

The Pioneer LX (to be deployed as ROBO-GUIDE), has a user manual which lists operating restrictions[1] and can be extended to include trip hazards. Whilst the Pioneer LX uses a laser scanner for object avoidance, there is still the possibility of a trip hazard. There are three possible sets of conditions when ROBO-GUIDE will stop during normal operation: (H1) When the laser scanner detects an obstacle (e.g. a person), the Pioneer LX will stop, becoming a trip hazard. (H2) ROBO-GUIDE will naturally come to a halt in populated areas during much of its operational life, for example when waiting for the lift, in the lift, or behind a door. In these cases ROBO-GUIDE will be entering a higher risk state, where it is a stationary trip hazard. (H3) Whenever the Pioneer LX encounters a person in its path, it will stop if it cannot find a path to go around. It is easy to manipulate this behaviour so that ROBO-GUIDE can be made to stop in a dangerous position, e.g. in front of the door to an office, therefore must be mitigated.

3. Linking Verification to Safety

Before ROBO-GUIDE can be safely deployed in a building, populated by unsuspecting people, its operation should be verified against a set of specifications.

3.1. Safety Specification

The limitations and states of ROBO-GUIDE are conditioned on the environment state. This can be written in terms of abstractions such as the vicinity of a door and associated safe position. Therefore ROBO-GUIDE requires an abstraction engine [6] to translate its continuous state (e.g map position) to a set of discrete abstractions. With the discrete abstractions defined, it is possible to use formal verification methods to prove the decision making logic of ROBO-GUIDE always adheres to a specification. Examples include: (1) ROBO GUIDE should never enter the Moving (clear) or Moving (hazard) states if it believes someone is riding on top of it. (2) ROBO-GUIDE should never enter the Permanent Park state when not in a safe position. (3) If ROBO-GUIDE is near a door, then at some point in the future, it must enter the Moving (hazard) or the Error (serious) state. (4) If ROBO-GUIDE encounters a failure in state transition, and remains in, either Error (serious) or Error (minor).

3.2. Performance Specification

In addition to ensuring ROBO-GUIDE performs safely in the environment, it is also important to know that it will complete its desired task successfully. One of the most challenging aspects of the task facing ROBO-GUIDE is the need to use a lift, with the help of unsuspecting humans. This challenge introduces additional specifications such as: (1) If ROBO-GUIDE is in the lift, it will, at some point in the future, be on the correct floor. (2) If ROBO-GUIDE is in the lift, it will, at some point in the future, not be in the lift. (3) If ROBO-GUIDE is not on the correct floor it will, at some point in the future, be in the lift. During the development of ROBO-GUIDE, it is necessary to ensure that all the discrete states that are important to safety or performance are determined and suitable specifications derived. This process will require the operation of ROBO-GUIDE in supervised tests allowing refinement of abstractions and specifications.

4. Safety Case: Safety to Specification

A safety case is a method for arguing, with evidence, that a system is safely operational within an environment [2,4],

[1] Pioneer LX User Manual

and to demonstrate how that safety has been achieved. Goal Structuring Notation (GSN) provides a method for arguing, in a "clear, comprehensible and defensible manner" that a system is safe to operate in a given context [2]. A GSN argument is composed using a standard symbol set [4].

4.1. Developing a GSN Pattern

This paper has considered hazards caused by the movement of a Pioneer LX deployed as ROBO-GUIDE in a crowded environment. The scenarios presented in Section 2 require mitigation in order to satisfy safe behaviour. Figure 1 shows a GSN pattern [3] for arguing the safety of ROBO-GUIDE in its operational environment using the GSN Standard [4]. By mitigating all of the hazards that are present within a Functional Hazard Analysis, captured by Context C2, the system can be assured to be functionally safe within the set operating environment, (shown by Goal G2); and therefore satisfies the overall claim in Goal G1 that it is safe to operate around a public inexperienced with autonomous robots, indicated in Context C1. Goal G3 reflects the need to avoid collision with humans under normal operation. Solution Sn1 presents information from verification techniques outlined in Section 3, to ensure the onboard sensors will provide general collision detection, and capture conditions under which this may not be so, mitigating Hazard H1.

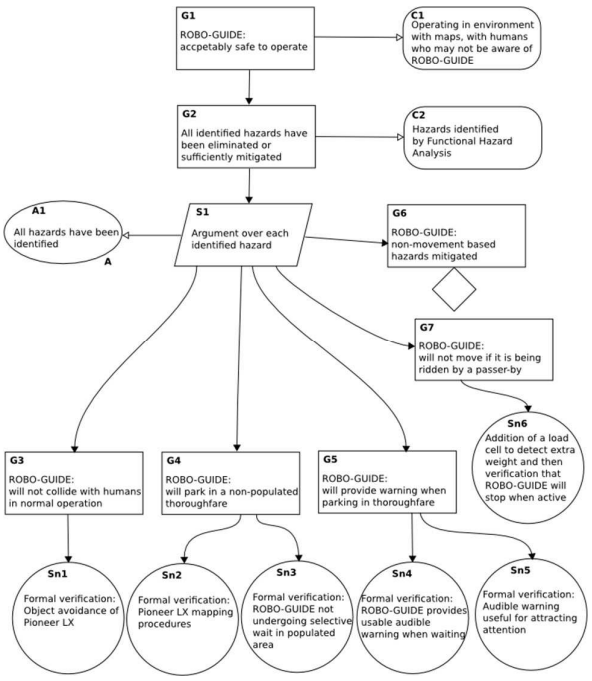

Figure 1. GSN Fragment for ROBO-GUIDE using the standard symbols set [4].

Undeveloped Goal G6, covers other hazards of movement not associated with collision, such as the drive-train becoming fouled. This can be accomplished using extra sensors to detect a fouled drive-train and verification to ensure that all motion is halted. One particular risk has been highlighted within the manual of the Pioneer LX. As it has a maximum capacity of 60 kg, no one may ride on top. In order to mitigate this, Solution Sn6 calls for a load cell to be added, and verification undertaken to prevent movement when overloaded. Goal G4 reflects the need of ROBO-GUIDE (when stopping) to park in a clear thoroughfare, so that it is out of the way of anybody passing through. The need to park in a clear thoroughfare is shown by Solutions Sn2 and Sn3. Hazardous areas of the map must be successfully identified, for example office doors (Sn2); mitigating Hazards H2 and H3. Given an understanding of hazardous areas of the environment from Sn2 verification techniques can be applied to ROBO-GUIDE to ensure it will never enter a waiting state in one of these regions (Sn3). Goal G5 reflects the need of ROBO-GUIDE to provide an audible warning to passers-by, when it waits in a thoroughfare. This is satisfied by Solutions Sn4 and Sn5, which will be influenced by the human-robot interaction components of ROBO-GUIDE [5].

5. Conclusions

This paper has outlined some potential hazards that a Pioneer LX may encounter when used as ROBO-GUIDE for leading members of the public around a set of office buildings. It has begun the process of identifying potential hazards associated with movement through the environment. To this end, the initial stages of a safety case have been outlined using GSN to record these possible hazards and link them to mitigation strategies.

References

1. Law J., Aitken J. M., Boorman L., Cameron D., Collins E. C., Chua A., Fernando S., Martinez-Hernandez U., McAree O. ROBO-GUIDE: Towards Safe, Reliable, Trustworthy, and Natural Behaviours on Robotic Assistants. Towards Autonomous Robotic Systems (2015) (in press)
2. Kelly, T., Weaver, R. The Goal Structuring Notation–A Safety Argument Notation. Proceedings of the Dependable Systems and Networks Workshop on Assurance Cases (2004)
3. Kelly, T., McDermid, J. Safety Case Construction and Reuse Using Patterns. In: Daniel, P. (ed.) Safe Comp 97, pp.55–69. Springer London (1997)
4. Origin Consulting Limited: GSN community standard version 1. Tech. Rep. (2014)
5. Cameron D., Collins E. C., Chua A., Fernando S., Martinez-Hernandez U., McAree O., Aitken J. M., Boorman L., Law J. Help! I Can't Reach the Buttons: Facilitating Helping Behaviors Towards Robots. Biomimetic and Biohybrid Systems (2015) (in press)
6. Dennis L. A., Fisher M., Lincoln N., Lisitsa A., Veres S. M. Declarative Abstractions for Agent Based Hybrid Control Systems. In: Declarative Agent Languages and Technologies VIII, pp. 96–111. (2011)