Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 96 (2016) 869 – 878

Procedia Computer Science

20th International Conference on Knowledge Based and Intelligent Information and Engineering Systems

A safety knowledge representation of the automatic driving system

Hiroyuki Utsunomiya[a]*, Nobuhide Kobayashi[a] Shuichiro Yamamoto[b]

[a]*DENSO CREATE INC. 3-1-1 Sakae Naka-ku, Nagoya Aichi 460-0008 Japan.*
[b]*Nagoya University Furo-cho Chikusa-ku, Nagoya Aichi 464-8601 Japan*

Abstract

With the development of technology and hardware, it has been assumed IoT(Internet of Things) society in the future that any device leads. In the automotive industry, in order to provide advanced services, such as automatic driving, any things are expected to lead the vehicle. In the IoT society, so that the lead is more than one system each other quality characteristics are different, such as safety. For this reason, there is concern that trouble is generated from the difference in the attitude toward safety. In order to prevent the problem is to visualize the design quality of each other's systems, it is necessary to obtain a common understanding among the developers.

In this paper, as a technique to visualize the design quality of the system, to create a description document of automatic operation system using the GSN(Goal Structuring Notation), to be able to objectively explained on the basis of the assumption and evidence the validity of the design quality of each other's system Check. Upon confirmation, provide a description items to be measures to hazards and threats that are expected in the relationship between the systems in automatic operation system, it showed the item should be explained to each other between the systems.

Such description structure is standardized, if shared between systems, with the common understanding can be obtained between developers can predict the quality required for the product. As a result, it is considered to be able to prevent a problem that occurs from the difference of the corporate culture.

Peer-review under responsibility of KES International

Keywords: GSN; HAZOP; FTA; hazard; threat

* Corresponding author. Tel.: +81-(0)52-238-0487; fax: +81-(0)52-238-0491.
E-mail address: HIROYUKI@dcinc.co.jp

Peer-review under responsibility of KES International
doi:10.1016/j.procs.2016.08.265

1. Introduction

In the future IoT society, in order to develop a high quality and safe system, it is essential to have obtained the common understanding for the quality and safety among the developers related to the development. For this purpose, it is necessary to document sufficient information capable of convincing the stakeholders and to visualize the design quality of the system.

In this paper, for the target of automatic driving system, we will organize the products and stakeholders leading to the automatic driving system to create a document explaining the safety (validity of quality) of each product among the developers using the GSN. We will clarify the process for creating an explanation document, and consider the explanation document to be required in the future IoT society. Discusses related research in Section 2, describes the safety of the description procedure of automatic driving system using the GSN in Section 3. We will add the discussions in Section 4, and finally make the summary and clarify the future challenges in Section 5.

2. Related work

Reference[1][5] describe notation of safety and dependability of the description document of the system. In this paper, we have adopted the GSN to the notation of the safety knowledge representation.

Reference[1][10][14] proposes knowledge system related to safety or dependability, but it does not provide a way to describe the GSN. Reference[3][4][5][6] proposes the notation or patterns related to a safety argument. However, it does not describe the relation between HAZOP(Hazard and Operability Studies), FTA(Fault Tree Analysis) and GSN. Reference[2][7][15] proposes the method combined HAZOP or FTA with D-Case(Dependability Case), but it does not describe the relation between HAZOP and FTA. Reference[8][9] shows the relation of safety analysis methods such as HAZOP, FTA, but it does not show the relation with GSN. Reference[11][12] proposes the method of generating safety case, but it does not describe concrete analysis methods such as HAZOP. Reference[13] proposes the method of generating D-Case based on Context Dependency Matrix. However, it does not consider about HAZOP and FTA.

Any of the research, the applied case to the automatic driving system are not included. Therefore, in the system development in the future of the IoT society, the safety knowledge representation of automatic driving system shown in this paper is considered to be effective.

3. Adopted safety analysis process

Here, we describe the procedure for creating an explanation document that the developers involved in the development of the automatic driving system confirm the quality of each other's product and verify the quality of the entire system.

(1) Define (Agree) the quality requirements the system should achieve.
(2) Organize the context such as the configuration of the target system.
(3) Confirm the quality of the system based on the context.

3.1. Defining the quality requirements the system should achieve

In the automatic driving system, various devices will be connected. Due to having been connected, threats such as the falsification of communication data are considered to increase. Furthermore, with the falsification or reception error of communication data, it is also conceivable that hazards may occur in the system. Here, hazard is due to the failure of internal systems, the threat is that it is assumed that due to attack from outside (malicious third party), which measures both the internal factors and external factors that impair the safety of the system, describing the quality of the entire system is appropriate:

(A) Countermeasures against the possible hazards have been established.
(B) Countermeasures against the possible threats have been established.