Hazard Analysis for self driving car system

K. K.
D.C. Nagoya, Japan
github:

O. K.
NMIRI
Nagoya, Japan
github: https://github.com/kaizen-nagoya/

***Streszczenie*—We try to update our hazard analysis system for self driving car system. UML, HAZOP and other methods and tools are applied.**

I. Introduction

A. What is HAZOP

In Quora.com, question and answer service in the net, there are some questions same as "What is HAZOP".

Some answer indicate IEC 61882[1] and others indicate wikipedia[2].

These are main explanations about HAZOP, respectively.

IEC: "This standard describes the principles for and approach to guide word-driven risk identification. Historically this approach to risk identification has been called a hazard and operability study or HAZOP study for short. This is a structured and systematic technique for examining a defined system, with the objectives of:"

There are 3 good points. 1st point is focusing on "guide word".

Guide word driven risk identification lies at the heart of HAZOP study. In other words, HAZOP is a guid word driven brainstorming at risk identification.

HAZOP guide words are highly abstract, so it can use any system levels of any systems.

11 guide words categorize space, time and others.

Space guide words are "more", "less", "as well as" and "part of". Time guide words are "early", "late", "before" and "after". Each guide word has a opposite pair, more and less, "as well as" and "part of", early and late, and before and after. more and less and early and late are quantitive.

Using TRIZ, guided brainstorming(tm) is popular in the manufacturing industry[3].

2nd point is risk identification. Risk handle not only negative issue, but also positive issue. Safety analysis should include negative and positive.

3rd point is "structued and systematic". The structure represents static and the system represents dynamic.

Wikipedia at Nov. 20, 2019 "A hazard and operability study (HAZOP) is a structured and systematic examination of a complex planned or existing process or operation in order to identify and evaluate problems that may represent risks to personnel or equipment."

There are 3 good points. 1st point is structured and systematic. same as IEC HAZOP.

From his, we can see HAZOP can handle static issue and dynamic issue. 2nd point is planned or existing. Planned is not yet

3rd point is personnel or equipment. HAZOP may be used focusing on only equipment. On a chemical plant, analysis target may be magnetic valves and their controllers. It is not good, because equipment is a part of system. Other many components of system should be considered. if an operator can control directly the system, analysis target should include the operator. If a control program can be changed by a programmer, analysis target should include the programmer. If an information of the system has an error, analysis target should include all information of the system. If an organization decide the operation process of the system, analysis target should include the process and organization.

B. TRIZ and HAZOP

The difference with TRIZ and HAZOP is complexity. TRIZ define many guide words such as 40 inventive principles[4].

TRIZ are used not only in physical system, but also in Information system [5], [6].

HAZOP guide word is

40 Principles (known solutions)

C. UML models

II. 3 phases

In HAZOP study, 3 phases are planed. 1st phase is before design, 2nd phase is after design and 3rd phase is before release.

A. unexpected problems

Before designing a product or services, unexpected design issue or unexpected operation should be listed at 1st phase.

B. coverall

At 2nd phase, design should review the design with coverage of all aspects.

C. unresolved issue

At 3rd phase, before release, unresolved issue should be listed. Some of them may described on the manual. Some of them may appear on the operation screen or errors and warnings. Others may be use training materials.

III. exercise session

HAZOP sessions are different directions on the phases. In a case, unexpected issues may list in 1st phase, in a case, unexpected issues may list in 2nd phase, and in a case, unexpected issues may list in 3rd phase depending the characteristics of the product and the services.

A. *typical session*

For unexpected issue, one typical HAZOP session is below.

1) 3 people are belong one group.
2) Having time to think and write on one person separately.
3) Having time to discuss within a group, the first report is from the person with the fewest items.
4) Report to all members what the most important issue the the group decide.
5) People are replaced by the method shown in the figure.

IV. Conclusion

We will try anything wha we can do.

Acknowledgment

We would like to thank to JASST, JAXA, IPA, and many people and companies who join safety analysis using HAZOP study.

Literatura

[1] IEC 61882: Hazard and operability studies (HAZOP studies) - application guide, IEC, 2016

[2] http://wikipedia.org/HAZOP/

[3] Extended 120 TRIZ Links in the World, nakagawa@ogu.ac.jp, https://www.osaka-gu.ac.jp/php/nakagawa/TRIZ/eTRIZ/elinksref/eWorldLinks.html

[4] 40 Inventive Principles of Automotive, The TRIZ Journal, https://triz-journal.com/40-principles-automotive/

[5] Inventions on Tree Navigators used in Graphical User Interface, Umakant Mishra, arXiv:1404.6756, 2014

[6] Inventions on dialog boxes used in GUI, Umakant Mishra, arXiv:1404.6754, 2014

[7] ingis, C., Liu, Y. From UML to design by contract. Journal of object-oriented programming, April issue: 6-9, 2001.

[8] tkinson, C., Bayer, J., Bunse, C., Kamsties, E., Laitenberger, O., Laqua, R., Muthig, D., Paech, B., Wüst, J., Zettel, J. Component-based product line engineering with UML. Addison-Wesley, 2002.

[9] órski J., Jarzębowicz A., Detecting defects in object-oriented diagrams using UML-HAZOP, Foundations of Computing and Decision Sciences, Vol. 27 (2002), No 4.

[10] . Jürjens. Developing safety-critical systems with UML. In P. Stevens et al., editors, Proceedings of UML 2003, volume 2863 of LNCS. Springer Verlag, 2003. http://www.isis.alexandra.dk/software, http://www.isis.alexandra.dk/software

[11] . Guiochet, G. Motet, C. Baron, and G. Boy. Toward a human-centered UML for risk analysis. In In WCC 18th IFIP World Computer Congress, Human Error Safety and System Development, 2004.

[12] uiochet, J., Baron, C.: UML based risk analysis - Application to a medical robot. Proc. of the Quality Reliability and Maintenance 5th International Conference, Oxford, UK, pp. 213-216, Professional Engineering Publishing, I Mech E. April, 2004 (2004)

[13] ansen, K. M., Wells, L., Maier, T., 2004. HAZOP analysis of UML-based software architecture descriptions of safety-critical systems. In: Nordic Workshop on UML and Software Modeling (NWUML04).https://www.researchgate.net/publication/249883238_HAZOP_Analysis_of_UML-Based_Software_Architecture_Descriptions_of_Safety-Critical_Systems

[14] orski, J., Jarzebowicz, A., 2005. Development and validation of a HAZOP- based inspection of UML models,. In: 3rd World Congress for Software Quality, Munich, Germany. https://www.researchgate.net/publication/241608330_Development_and_validation_of_a_HAZOP-based_inspection_of_UML_models

[15] o with the Early Bird http://jasst.jp/archives/jasst07e/pdf/D2-3.pdf(Japanese only) https://tech.nikkeibp.co.jp/dm/article/HONSHI/20061019/122445/

[16] wu, F., Galloway, A., Mcdermid, J., Ian, T., 2007. Integrating safety and formal analyses using UML and PFS. Reliability Engineering and System Safety 92 (2), 156-170. https://www.sciencedirect.com/science/article/pii/S095183200500270X

[17] artin-Guillerez, D., Guiochet, J., Powell, D., Zanon, C.: A UML-based method for risk analysis of human-robot interactions. 2nd InternationalWorkshop on Software Engineering for Resilient Systems, pp. 32-41 (2010)

[18] azard analysis of human-robot interactions with HAZOP-UML, Jérémie Guiochet, University of Toulouse, LAAS-CNRS, Toulouse, France, Safety Science, Elsevier, 2016, 84, https://arxiv.org/pdf/1602.03139.pdf