DOI:10.19026/rjaset.16.5387
ISSN: 2040-7459; e-ISSN: 2040-7467
© 2019 Maxwell Scientific Publication Corp.
Submitted: February 25, 2019 Accepted: March 27, 2019 Published: December 15, 2019

Research Article
Model-Based Functional Safety Analysis of Manufacturing Processes for Weapon Systems

Jae-Chul Kim, Young-Min Kim and Jae Lee
Department of Systems Engineering, Ajou University, Suwon, Republic of Korea

Abstract: The present study aims to propose a method of carrying out the functional safety analysis to ensure the safety of the manufacturing process for weapon systems. The purpose of using weapon systems is to harm human life and destroy the property of hostile countries. Naturally, a weapon system involves explosives during its development and operation. As such, manufacturing processes for weapon systems have potential hazards of accidents that can cause fatal damages to humans or property. Some erroneous activities in the manufacturing process can produce dangerous results. For this reason, the safety of manufacturing processes in the defense industry domain is more crucial than other general manufacturing domain. To deal with such a safety issue, in this research, we propose a model-based approach to ensuring the safety of the manufacturing process for the defense industry. The proposal is primarily based on the concept of functional safety and includes the three steps: determination of safety integrity levels; selection of appropriate safety analysis methods; and execution of the analysis methods using SysML models. Using the results obtained in the study, one can identify the risk factors in a complex manufacturing environment in advance to take preventive actions against the potential loss that may arise.

Keywords: Defense industry, manufacturing process, model-based safety analysis, system modeling language (SysML), system safety

INTRODUCTION

A primary target of the defense industry domain is the development and production of weapon systems aimed at harming human life and destroying property. Naturally, weapon systems involve explosives during the development and operation of them. As such, the manufacturing process of the weapon systems has a risk that workers at the production lines are exposed to a potential explosion. For this reason, the safety of manufacturing processes in the defense industry domain is more critical than other general manufacturing domain.

The manufacturing process of the weapon system tends to ensure safety through automation. However, the safety in the automation of the manufacturing process must be dealt with the primary risk of the manufacturing process as well as the risk associated with the automation of the equipment with the operation process. As the weapon system is involved, the subject of safety analysis is also getting complicated.

Recently, in the manufacturing field, there are many changes due to the 4th Industrial Revolution that utilizes IOT and sensor technology and so forth (Lasi et al., 2014). To study how to ensure the practical application of these technologies, many researchers have published about the functional safety of manufacturing processes and machinery. These research results made it possible to allow a class of international standards on functional safety (IEC 62061, IEC 61511 and ISO 26262 and others) to be related to the functional safety of various automation factories (Meany, 2017). Therefore, in this study, we propose a research method to effectively perform a functional safety analysis of the manufacturing process of the weapon system.

LITERATURE REVIEW

Over their long life, weapon systems involve many people such as developers, manufacturers and users. Most munitions contain explosive materials that, upon accidental initiation, may result in hazards to human life and property within the explosion radius. So safety is a crucial issue during weapons lifecycle (Terenowski and Krzyński, 2017).

In the defense industry, the MIL-STD-882 defines many safety-related programs. However, the standard focuses on the safety activities of the system's function and function development process. For this reason, the safety of the manufacturing process follows the
Due to the increased complexity of modern systems, related processes are also getting complicated. In keeping pace with the trend, the automation with the processes and equipment needs to be more sophisticated (Dahn and Laughery, 1997; Bunting and Belyavin, 1999). On the other hand, safety processes require appropriate safety analysis methods. For these reasons, there has been much research on a variety of ways for safety analysis of the complex systems development (France and Rumpe, 2007; Papadopoulos et al., 2001; Guiochet, 2016). In particular, Mhenni et al. (2013) conducted a study to ensure safety by using the SysML-based model and using the linkage between the attribute information of the system and the attribute information of the safety analysis method. Also Jung and Lee (2014) conducted research that applies to functional safety analysis based on SysML-based (ISO 26262, 2011) specifications.

The purpose of this study is to propose a method to carry out the functional safety analysis for ensuring the safety of the manufacturing process of the weapon systems. To achieve a goal of the research, we employ a Model-Based Safety Analysis (MBSA) and evaluation Safety Integrity Level (SIL) to generate a failure model that accurately incorporates the failure information.

MATERIALS AND METHODS

SIL Concept: The functional safety standards state that different design approaches are used based on the Safety Integrity Level (SIL Level) to evaluate the safety of Electrical and Electronic (E/E) components constituting an automobile, safety of related parts. The criteria for determining the SIL for the analysis and evaluation of the safety associated with the IEC 62061 based manufacturing process are as follows (Fuches and Zajicek, 2013).

IEC 62061-based Class of probability (Cl) is evaluated according to the formula described in Table 1, where Frequency and exposure time (Fr), Probability of occurrence (Pr) and Possibility of avoiding or limiting harm (Av) elements.

The SIL can be classified from grade 1 to grade 3. In the case of SIL 2 to 3, it is a specification that requires careful attention to ensure more safety. (IEC62061 and IEC61511 (International Standard for Safety Consistency Evaluation (SIL Level)) as shown in Table 2, respectively (IEC 62061, IEC61511).

Functional safety and ISO 26262: The meaning of safety is the protection from the risks of health and economic loss. However, in ISO 2626 (IEC 61508, 2010), safety is a state that there is no risk not reasonable or unacceptable. There are many unexpected risks such as natural disasters that can be faced when we use a car. However, many risks can be reduced in the functional aspect of the development phase. The range of safety that a vehicle developer or producer must deal with a functional perspective. Moreover, the functional safety specified by the ISO 26262 standard is to guarantee the functional safety of Electrical and Electronic (E/E) devices (Cho et al., 2009).

In the field of manufacturing, efforts are being made to ensure the functional safety of the electrical and electronic (E/E) domain following the enhancement of production automation. The IEC 62061 and IEC 61511 are the functional safety international standards in the general manufacturing domain. The automotive industry stipulates ISO 26262, the international standard for functional safety of automobiles, to ensure safety with the increase in the complexity of automobile functions over the last decade, thereby providing functional safety.

The purpose of ISO 26262 is to design a resource that identifies the source of the risk and reflects the results of the risk analysis activities based on HARA (Hazard Analysis and Risk Assessment) analysis activities to ensure safety. ISO 26262 differs from the functional safety standard of the general manufacturing industry (IEC 62061/IEC 61511) in that it defines the use of semi-formal notation as a model-based analysis and design method (ISO 26262, 2011).

SysML (Systems Modeling Language): SysML is a modeling language developed for data interchangeability and reusability, which prevents the interpretation of the system related to the development of the system. Table 3 describes the characteristics of SysML (Kim and Lee, 2012).

As can be seen in the SysML diagram type in Fig. 1, SysML consists of three categories of behaviors, requirements and structure diagrams.

The characteristics of each diagram can be described as follows (Friedenthal et al., 2014):

- ‘Package Diagram’ organizes model elements in a model in terms of packages. (Same as UML package diagram.)
Table 3: Characteristics of SysML (Friedenthal et al., 2014)

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard language</td>
<td>- Easy to share information</td>
</tr>
<tr>
<td></td>
<td>- Same understanding possible between different stakeholders</td>
</tr>
<tr>
<td></td>
<td>- Compatibility</td>
</tr>
<tr>
<td></td>
<td>- An explicit representation of the system</td>
</tr>
<tr>
<td>Graphical modeling language</td>
<td>- Enable more effective communication of target systems</td>
</tr>
<tr>
<td></td>
<td>- Can be segmented and layered by various relationships such as structure and behavior</td>
</tr>
<tr>
<td>Compacted language specification</td>
<td>- More compact and easier to understand than UML</td>
</tr>
<tr>
<td>Traceability</td>
<td>- Easy to design change and problem identification</td>
</tr>
</tbody>
</table>

Fig. 1: Structure of SysML (Friedenthal et al., 2014)

- ‘Requirement Diagram’ includes text-based requirements and their relationship with other requirements, design elements and test cases to support requirements traceability. (Not in UML.)
- ‘Activity Diagram’ models how the target behaves in an orderly fashion. Note which actions are executed depends on the availability of their inputs, outputs and control and how the actions transform the inputs to outputs. (Modification of UML activity diagram.)
- ‘Sequence Diagram’ represents behavior in terms of a sequence of messages exchanged between systems, or between parts of systems. (Same as UML sequence diagram)
- ‘State Machine Diagram’ represents the behavior of an entity in terms of its transitions between states triggered by events. (Same as UML state machine diagram)
- ‘Use Case Diagram’ represents functionality in terms of how a system is used by external entities (i.e., actors) to accomplish a set of goals. (Same as UML use case diagram)
- ‘Block Definition Diagram’ represents structural elements called blocks and their composition and classification. (Modification of UML class diagram)
- ‘Internal Block Diagram’ represents inter-connection and interfaces between the parts of a block (modification of UML composite structure diagram)
- ‘Parametric Diagram’ represents constraints on property values, such as $F = m*a$, used to support engineering analysis. (Not in UML)

**RESEARCH METHOD**

In this study, we propose a method of ensuring safety using the model-based method by the three-step procedure to achieve the research goal. Figure 2 shows a procedure for the proposed method of ensuring safety using the model-based method.

**Step 1:** Evaluate SIL based on a comprehensive consideration of the risks of equipment, machinery and manufactured products in the defense industry. Also, select a safety analysis method that should be performed based on the SIL evaluation.

**Step 2:** Analyze the characteristics and capability of the individual safety analysis method. Also, select the appropriate SysML diagrams that can be used with the studied safety analysis methods for the process/machinery safety.
**Step 3:** Derive the safety requirements for the process or machinery based on the results of the safety analysis. Safety requirements shall be taken to ensure the safety of process and machinery equipment.

**RESULTS AND DISCUSSION**

**Case study:** The research method proposed in the previous section was applied to the safety design of solid propellant (Fig. 3). First, we evaluated the SIL of
each process for manufacturing the solid propellant. Then, we then selected safety analysis methods and conducted them for the safety of process, machinery and products. For this purpose, Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) methods had been selected as the safety analysis method corresponding to SIL 3-4. Safety analysis method FMEA and FTA are the methods that are performed for the safety analysis of the model for SIL3-4.

After that, safety analysis was conducted through the SysML of the attribute information of the main processes of the solid propellant which have the process and machine aspects.

The manufacturing process of the solid propellant can be divided into three steps as shown in Fig. 4.

In this section, we applied the research method the following three steps established in the previous section.

**Step 1: SIL evaluation:** As described in the previous chapter, the evaluation of the SIL depends on the sum of the indicators of the likelihood of occurrence of the risk (CL) and severity. In this case study, we identify the primary risk of the solid propellant manufacturing process and evaluated by the evaluation standard of IEC 62061 as shown in Fig. 5. In the evaluation results, the P2 process was identified as the SIL3 evaluation and the safety analysis was performed.

**Step 2: Selection of safety analysis method:** MIL-STD-882E (2012) the safety standard for the defense industry, focuses on development-related activities. Instead, the activity related to the manufacturing process is limited to the control of dangerous materials. Thus, we considered Hazard and Operability analysis (HAZOP), FMEA and FTA presented in IEC 61508, IEC 62061 and IEC 61511 that are the functional safety standard in general manufacturing domain. We selected both FMEA and FTA to be used as a safety analysis
Step 3: Model-based safety analysis: The modeling language used in this research is SysML. SysML can be used to describe the dynamic information of the system and the structural information. By using SysML, (Helle, 2012) conducted a study to provide a methodology and tool support for an integrated MBSE and MBSA on one common model based on SysML. According to this study, we could analyze the dynamic information and the structural information of safety for the solid propellant manufacturing process. In this study, we have established a methodology using five diagrams to identify information related to the process and machine characteristics of the nine figures provided in SysML.

Based on this, the results of analysis using SysML were reflected in FMEA and FTA as follows.

In general, safety analysis activities should be able to predict the possible failures and evaluate their following effects. In solid propellant manufacturing processes, there are many risks due to the characteristics of the weapon system. So, we used SysML to model the static aspects such as process equipment and the dynamic elements such as the operation of the operator by using the various diagrams that were specified in Table 4. In this manner, we used the information on model-based safety analysis to apply to safety analysis.

Figure 6 shows the result of structural analysis of batch mixer that facility of the case study process.

Figure 7 shows the scenario of the process with the worker. As shown in Fig. 7, use-case diagram is useful to analyze process functions.
Table 4: Selection of SysML diagrams for different safety analysis methods

<table>
<thead>
<tr>
<th>Analysis type</th>
<th>SysML diagram</th>
<th>Safety analysis method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Structure analysis</td>
<td>Block definition diagram</td>
<td>FMEA</td>
</tr>
<tr>
<td>Functional analysis</td>
<td>Use-case diagram</td>
<td></td>
</tr>
<tr>
<td>Malfunction analysis</td>
<td>Activity diagram</td>
<td></td>
</tr>
<tr>
<td>Effects analysis</td>
<td>Sequence diagram</td>
<td></td>
</tr>
<tr>
<td>Top-event identify</td>
<td>Use-case diagram</td>
<td></td>
</tr>
<tr>
<td>Basic event identify</td>
<td>Activity diagram</td>
<td></td>
</tr>
</tbody>
</table>

Figure 7: Use-case diagram of the case study (partial)

Figure 8 shows the behavior in terms of a sequence of messages exchanged between each process. In this study, we performed FMEA for the manufacturing process of the solid propellant. Table 5 summarizes the FMEA results for this process.

Validation of the results: In this study, we have extended the categories of safety analysis categories that can be generated in the field of manufacturing through research. Moreover, based on this, we have identified the risks of the operational viewpoint of the manufacturing process.

Notably, in the traditional safety analysis method, the risk or hazard was identified by using the brainstorming and the past information. However, in this research, we have identified those risks through the main categories such as process, equipment and operation. As a result, we complemented the existing safety analysis and confirmed that it could be used in the manufacturing domain of the weapon system.

CONCLUSION

Today's defense industry also tends to automate processes in response to the development of manufacturing technology. Moreover, it is difficult to ensure safety in such changes. In this study, we aimed to secure safety by building model based safety analysis methodology applicable to the defense industry. For this purpose, SysML was used to construct a method of ensuring the safety of the manufacturing process of the defense industry through static and dynamic aspects.
Table 5: FMEA result of the case study (partial)

<table>
<thead>
<tr>
<th>Process</th>
<th>Failure mode</th>
<th>Effect</th>
<th>Recommended action</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pouring raw material</td>
<td>Ingress of dirt and debris</td>
<td>Performance degradation</td>
<td>Install filter</td>
<td>Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Explosion in mix process</td>
<td>Construction of dustproof environment</td>
<td>Tool</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Use of spark-free equipment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Creating a vacuum environment</td>
<td></td>
</tr>
<tr>
<td>Mixing raw material equally</td>
<td>Generate bubbles in the slurry</td>
<td>Performance degradation</td>
<td>Install filter</td>
<td>Environment</td>
</tr>
<tr>
<td></td>
<td>Ingress of dirt and debris</td>
<td></td>
<td>Construction of dustproof environment</td>
<td>Tool</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Use of spark-free equipment</td>
<td></td>
</tr>
</tbody>
</table>

This research is expected to contribute to ensuring the safety of factory automation construction and operation in the defense domain in the absence of a separate international standard for ensuring the safety of manufacturing process in the defense industry.

CONFLICT OF INTEREST

It should be noted that there is no financial support and there is no competitive interest in this area.

REFERENCES


