Risk Assessment of RCCS by Applying FMECA
Quantitative Analysis

Hojin Yoon
Department of Computer Science and Engineering, Hyupsung University,
Hwaseung, Kyunggido, South Korea
hjyoon@uhs.ac.kr

Abstract. Safety Critical System (SCS) requires Risk management. SCS is a
system, whose failure might endanger human life, leads to substantial economic
loss, or causes extensive environmental damage. Risk management is necessary
in SCS since risk would threaten system Safety. For the effective management,
risk needs to be assessed through an authorized risk mode, such as FMEA, FTA,
or FMECA. FMEA is especially for Embedded system, which SCS is classified
in. And adding Criticality to FMEA, FMECA was defined. We apply FMECA to
Railroad Crossing Control Critical System (RCCS), and analyze the quantitative
result. It would show how a risk model works in risk management of SCC.

Keywords: Risk Assessment, FMECA, Safety Critical System

1 Introduction

Risk threatens Safety [1], which is one of the most critical quality in Safety Critical
System (SCS). At first, we mention Risk- related terms according to Koopman’s[2].
Hazard is a situation with potential danger to people, environment, or material. For
example, an interlock, which is supposed to prevent subway door from opening, isn’t
activated. Incident is a situation with actual danger to people, environment, or material.
Sometimes a hazard results in an incident. But it is not going to an accident. It is near
miss. In the case of the interlock’s hazard explained above, subway door opens, but
nobody is leaning against it. Sometimes, an incident would turn into an accident. Accident
is an event that cause death, injury, environmental or material damage. In the
case of the interlock above, subway door opens, and someone falls out of car. Accident
is called Mishap.

Risk is in a level of Hazard in terms of its potentiality. Hazard would go to incident
or accident. The possibility of a hazard-to-accident and the impact of its accident are
assessed for the effective Risk management, and most of risk models measure the
possibility and the impact. Normally, the multiplication of the possibility and the impact
represents Risk Exposure value. But some models add their unique factors, which
measure some other qualities Risk management should care for a special purpose. In
this paper, we analyze Railroad Crossing Critical System (RCCS) through Failure
Mode and Effects Criticality Analysis (FMECA), which measures Criticality as well as
the possibility and the impact in its quantitative analysis.
This paper applies FMECA, the most delicate risk model, to RCCS, which has been widely used in conventional SCS research. Sections 1 and 2 explain FMECA and RCCS, and Section 3 describes the application of RCCS’s FMECA quantitative analysis. Section 4 concludes the findings of this work.

2 Related Research

2.1 Risk Assessment

Risk model measure how risk in real a risk would be. It is called Risk Exposure (RE), which is normally computed by multiplying Probability and Impact. The probability means the possibility where a potential risk results in an accident (or mishap), and the impact means how severe the accident is in the system failure. The higher RE a risk has, the more strongly its mitigation activity should be conducted [3]. This mitigation activity avoids the accident that would be caused from the risk.

Probability and Impact are scored by an expert, and this scoring system is based on ordinal scale [4]. Ordinal scale represents the relative order of objects; Star rating is one of the popular ways using ordinal scale. It could depend on who scores. Recovering this lack of objectiveness of ordinal scale, some authorized organizations provide a standard table for Probability or Impact as a reference. For instance, National Institute of Standardization and Technology (NIST) has published a guideline for information systems [5], and Department of Defense (DoD) has provided a guideline for SCS [6]. Figure 1 is NIST version for Impact, and Figure 2 is DoD version for Impact.

<table>
<thead>
<tr>
<th>Impact Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
</tr>
<tr>
<td>Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization’s mission, reputation, or interest; or (3) may result in human death or serious injury.</td>
</tr>
<tr>
<td>Medium</td>
</tr>
<tr>
<td>Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization’s mission, reputation, or interest; or (3) may result in human injury.</td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization’s mission, reputation, or interest.</td>
</tr>
</tbody>
</table>

Fig. 1. Guideline for Scoring Impact in NIST 800-30 [7]
2.2 Failure Mode and Effects Criticality Analysis

FMECA was developed by the National Aeronautics and Space Administration (NASA) to verify and improve the reliability of the aerospace program’s hardware. A sub-committee consisting of representatives from government, industry, and academic circles created FMEA based on the MIL-STD 1692, a project which was cancelled in 1998 [7]. As the most commonly used method in embedded system design, FMEA is a technology for analyzing the consequences of system failure, and it requires a domain expert. FMECA is a combination of FMEA and criticality analysis, which allows for more complex measuring of risk factors. Its use is highly recommended in the industry [8].

In FMECA, an overall assessment of criticality is the key. Criticality could be another name of RE. It is calculated through a complex analysis named “Quantitative analysis” while RE is a multiplication of Probability and Impact. Quantitative Analysis measures Mode Ratio, Probability of Loss, Mode Criticality, and Item Criticality. FMECA is perceived as giving more accurate values than FMEA. In this research, we analyze RCCS using FMECA as the risk model.
3 RCCS Quantitative Analysis

3.1 Railroad Crossing Critical System

The Railroad Crossing Critical System (RCCS) is a system designed by Medikonda to analyze safety in his thesis [9]. It is also being used in other research papers on safety to explain their suggested technologies. RCCS is a prototype implementation that controls gates in a railroad crossing. It lowers the gate to block the crossing before the train reaches it, and it raises the gate after the train has passed.

The main inputs to the control system are scattered across the track circuit in seven sensors; two crossing gates at the crossing known as Gate 1 and Gate 2, a track change switch, and three signal lights. The output is the train, Gate 1, Gate 2, the track change switch, and the control signal for the signal lights. RCCS is designed to have the following functions described in Table 1.

Table 1. RCCS System Functions [9]

<table>
<thead>
<tr>
<th>RCCS System Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control the overall operation of train on the track circuit</td>
</tr>
<tr>
<td>Control the opening and closing of Gate 1 and 2 at the railroad intersections</td>
</tr>
<tr>
<td>Control the track lever to change the track route from the outer to the inner loop</td>
</tr>
<tr>
<td>Check the internal health of all the subsystems</td>
</tr>
<tr>
<td>Control the train operation at the Signal Lights</td>
</tr>
<tr>
<td>Monitor all the sensors on the track circuit</td>
</tr>
</tbody>
</table>

3.2 Quantitative Analysis

The quantitative analysis of criticality calculates the risk exposure for each of the hardware items through a series of equations. It can be applied to prioritize risk management activities. The following equations are applied, and then the hardware items and failure modes are listed according to their risk values. Mode Criticality is calculated by multiplying λp, t, Mode Ratio, and Probability of loss. This evaluates how critical a specific failure mode is. Mode criticality is calculated with the following equation:

\[
\text{Mode Criticality} = \text{Expected Failure (for the item)} \times \text{Mode Ratio (for the failure mode)} \times \text{Probability of Loss (for the failure mode)}
\]

Item Criticality is the sum of all criticalities for each failure mode for a given item. Table 2 is the result of conducting Quantitative Analysis over RCCS.
Table 2. Mode Criticality and Item Criticality in RCCS

<table>
<thead>
<tr>
<th>Item</th>
<th>Failure Modes</th>
<th>Mode Criticality</th>
<th>Item Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor</td>
<td>F1.1</td>
<td>5.5188</td>
<td>9.4608</td>
</tr>
<tr>
<td></td>
<td>F1.2</td>
<td>3.942</td>
<td></td>
</tr>
<tr>
<td>Warning Lights</td>
<td>F2.1</td>
<td>87.6</td>
<td>175.2</td>
</tr>
<tr>
<td></td>
<td>F2.2</td>
<td>87.6</td>
<td></td>
</tr>
<tr>
<td>Gate</td>
<td>F3.1</td>
<td>6.3072</td>
<td>33.9012</td>
</tr>
<tr>
<td></td>
<td>F3.2</td>
<td>7.884</td>
<td></td>
</tr>
<tr>
<td></td>
<td>F3.3</td>
<td>19.71</td>
<td></td>
</tr>
<tr>
<td>Controller</td>
<td>F4.1</td>
<td>43.8</td>
<td>43.8</td>
</tr>
</tbody>
</table>

4 Conclusions

RCCS was assessed through Quantitative Analysis of FMECA. The system has four hardware items and it 8 failure modes totally. Quantitative analysis first defines Mode Ratio for a failure mode. The sum of ratios for each item is supposed to be 100% according to the model. It corresponds to Impact in RE. And Probability of Loss is necessary for calculating Mode Criticality as shown in Section 3. If Probability of Loss is 100%, failure of the item must result in system failure. It corresponds to Probability in RE. We calculated Mode Criticality and Item Criticality in Table 2.

The mode criticality of the failure mode for F1.1 is 5.51, which is higher than that of F1.2, but much lower than for other failure modes. In the case of F2.2, when the controller malfunctions, the criticality is at a high value of 82.6, meaning that more central risk management needs to be taken for the controller as compared to the failure mode of F1.1.

Now, we extend the result by adding Qualitative Analysis of FMECA, and define the association relations between factors included in each analysis. In future, we will set up the cross reference guideline of the factors for recovering ordinal scale’s limitation.

Acknowledgements. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2014R1A1A3051827).

References