Programming Guidelines for FBD programs in Reactor Protection System

Sejin Jung, Dong-Ah Lee, Eui-Sub Kim, JunBeom Yoo and Jang-Soo Lee
Dependable Software Laboratory
Konkuk University, Republic of Korea
Contents

• Introduction

• Background

• Guidelines for FBD programming
  – Guidelines
  – FBDChecker
    • Case study

• Conclusion
Introduction

• Safety critical systems are using FBD (Function Block Diagram) to design software
  – It used PLC (Programmable Logic Controller) programming language in plant automation industry

• FBD has several elements of making errors by human errors
  – Guidelines for reducing errors is needed

• Several guidelines for FBD programming exist
  – There are Some kinds of elements which need to modify and specify
  – We propose refine and added guidelines for FBD programming
Introduction

• CASE tool: FBDChecker
  – It check FBD programs for finding violations about guidelines
  – It uses standard input format of FBD
    • Standard XML format of FBD (PLCopen)

• Case study about FBDChecker
  – Example: 5 logics in BP of RPS
    • Finding violations in programs
Background – Function Block Diagram

• Function Block Diagram defined in IEC 61131–3 standard
  – Defined all function blocks and 10 categories

• FBD consists of number of function blocks
  – Interconnections between function blocks
Background – safe programming guidelines

- Safe Programming Guidelines
  - Programming guidelines for achieving safety of software
  - MISRA-C for development in automotive industry
  - DO-178B for airborne systems
  - NUREG/CR-6463 for development in nuclear domain
    - Contains IEC 61131-3 programming language, c/c++, Ada, Pascal, PL/M
Guidelines for FBD programs

• Making rules with two categories
  – Reliability
  – Maintainability

• Reliability
  – Rules about improving dependability and to guarantee correctness about simulation or action of a program

• Maintainability
  – Rules about increasing readability and decreasing complexity
Guidelines for FBD programs

• Reliability
  – Execution order
    • Using correct execution order
  – Eliminating incorrect move block
    • Connection between move block and function
  – Implicit/explicit type conversion
  – Variable initialization
    • Variable must be initialization before uses
  – Etc.
Guidelines for FBD programs

- Examples
  - Incorrect execution order
Guidelines for FBD programs

• Maintainability
  – Naming convention
    • Recommend additional identifier
    • Length – too short, too long

  – Diagram
    • Eliminating crossed lines
    • Eliminating overlapped blocks

  – Etc.
Guidelines for FBD programs

• Examples
  – Illegible diagram
Guidelines for FBD programs

• Comparison with existing guidelines and researches

<table>
<thead>
<tr>
<th></th>
<th>FBDChecker</th>
<th>NUREG/CR-6463</th>
<th>Research1</th>
<th>Research2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</td>
<td>FBD</td>
<td>FBD</td>
<td>FBD</td>
<td>IEC 61131-3</td>
</tr>
<tr>
<td>Diagram</td>
<td>O</td>
<td>O</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Data Type</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>△</td>
</tr>
<tr>
<td>Function using</td>
<td>O</td>
<td>△</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Automation</td>
<td>O</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>note</td>
<td>Need specify</td>
<td>5 case of guidelines</td>
<td>Target is not just FBD</td>
<td></td>
</tr>
</tbody>
</table>

Research1: Guidelines for the Use of Function Block Diagram in Reactor Protection Systems, accepted APSEC 2014
Research2: Restricting IEC 61131-3 Programming Languages for use on High Integrity Applications ETFA 2008
Guidelines for FBD programs

- Classification of rules
  - Two kinds of classification

- Warnings
  - Rules may have possible to errors
  - Illegible diagram
  - Explicit type conversion
  - Etc.

- Errors
  - Rules may make critical errors directly
  - Execution order
  - Initialization
  - Implicit type conversion
  - Etc.
Guidelines for FBD programs

• Compiling a list about guidelines using XML

```xml
<Chapter>
    <chapterName>Reliability</chapterName>
    <chapterNumber>1.1</chapterNumber>
    <ruleNumber>0</ruleNumber>

    <chapterName>Control flow</chapterName>
    <chapterNumber>1.1.1.1</chapterNumber>
    <ruleNumber>4</ruleNumber>
    <chapterContents>recommend not to use jmp</chapterContents>
    <explain>jmp makes difficult to understand control flow, so we re
```
FBDChecker

- **CASE tool**: FBDChecker
  - Automation tool for checking FBD programs about our guidelines
  - uses standard input format of FBD(PLCopen)
  - checks FBD programs

![FBDChecker Diagram]

- File path
- Operation button
- Kinds of filters
- Position information about violation blocks
- Contents about violations
FBDChecker

• FBDChecker uses information of FBD programs in XML proposed by PLCopen
  – Parsing xml and searching violations using information about position, type, connection, etc.

```xml
<block height="80" localId="2"
  typeName="AND_BOOL_2" width="90">
  <position x="710" y="1435"/>
  <inputVariables>
    <variable formalParameter="IN1" negated="false">
      <connectionPointIn/>
      <relPosition x="-1" y="-1"/>
      <connection
        formalParameter="OUT" refLocalId="1"/>
      </connectionPointIn>
    </variable>
    <variable formalParameter="IN2" negated="true">
      <connectionPointIn/>
      <relPosition x="-1" y="-1"/>
      <connection
        formalParameter="out" refLocalId="7"/>
      </connectionPointIn>
    </variable>
  </inputVariables>
  <inputOutputVariables/>
  <outputVariables>
```
Case study

- Filtering screen of POU
Case study

- Did case study about 5 logics in BP of RPS
  - Finds 18 kinds of and 264 numbers of violations
    - Type conversion
    - Illegible diagram
    - Naming
    - Etc.
Case study

- An example of a part of diagram in a logic
  - Too far block
  - Crossed line
  - Type conversion
Conclusion & Future Work

• Guidelines
  – We make guidelines which are refined and added

• CASE tool: FBDChecker
  – It uses standard XML format of FBD
  – It finds violations about guidelines which we proposed

• Future Work
  – Implement the improved FBDChecker for expansion easily about guidelines
  – Perform the Case Study about other logics
THANK YOU