Use of STPA in digital instrumentation and control systems of nuclear power plants

Martin Rejzek

Second European STAMP Workshop
22.09.2013 Stuttgart, Germany
Agenda

- Project background and objectives
- System under consideration
- Analysis approach
  - Process towards the hierarchical control structure
  - STPA step 1 and 2
  - Blended approach
- Conclusion and outlook
Project Background

- Replacement of existing instrumentation and control system (I&C system)
- Simultaneous transition from analog to digital system

How can STPA be efficiently applied to an I&C system as it is used in nuclear power plants?
Project Objectives

- Develop process to «transform» an I&C system specification into a hierarchical control structure
- Investigate potential of STPA (with respect to nuclear power plant I&C systems) by performing a case study
- Investigate potential to integrate existing analyses (FTA, ETA, FMEA, ...) into STPA (blended approach)

→ Detailed documentation
→ Case study
→ Knowledge transfer
System Under Consideration - Selection of the Case Study

1 Reactor
2 Steam generator
3 Reactor coolant pump
4 Pressuriser
5 High-pressure turbine
6 Water separator
7 Superheater
8 Low-pressure turbine
9 Condenser
10 Condensate pump
11 Low-pressure preheater
12 Feedwater tank
13 Feedwater pump
14 High-pressure preheater

Feedwater level control

Exemplary illustration
Information sources used:

- Facility documentation
- System specifications (level 3 & 4 documents)
- Manuals
- Expert knowledge
A generic way to represent a control function:

Sensor → Logic → Output

Case Study - System Architecture

Not what you want to start with!
Problem of Terminology - Functional Entities

Is this a

- function,
- module,
- sub-system,
- class,
- component, …?
Identification of Controllers -
What is a controller in the sense of STPA

Does functional entity …

• bear responsibility for a part of the process?
• possess necessary means to interact with process?
• receive necessary feedback for adequate control?
Recombination of Functional Entities - First Step towards the HCS

Exemplary illustration
Hierarchical Control Structure

- Setpoint controller
  - Low-load valve controller
  - Full-load valve controller

Level regulation with low-load valve
Steam generator feedwater level regulation
Level regulation with full-load valve
Project Objectives - A First Conclusion

✓ Develop process to «transform» an I&C system specification into a hierarchical control structure
  • Systematic and reproducible process
  • Could be partially automated
  • Basis: System Specification with additions

• Investigate potential of STPA by performing a case study

• Investigate potential to integrate existing analyses (FTA, ETA, FMEA, ...) into STPA (blended approach)
STPA Process - Step 1

1. Define Analysis Scope
2. Develop Hierarchical Control Structure
3. STPA Step 1

- Unsafe Control Actions
- Safety Requirements
- Existing Mitigation Measures
- Safety Assessment Design Level
- Coverage Report

© by ZHAW, Martin Rejzek, 2014
STPA Process - Step 2

Start

Define Analysis Scope

Develope Hierarchical Control Structure

Hierarchical Control Structure

STPA Step 1

STPA Step 2

Unsafe Control Actions

Scenarios

Safety Requirements

Existing Mitigation Measures

Coverage Report

Safety Assessment Design Level

Control Action (CA) Keyword
Unwanted Process Reaction (UPR)
Scenarios leading to \(\{\text{UPR}\}\) ?

Scenarios resulting in \(\{\text{CA}\}\) \(\{\text{Keyword}\}\)?
STPA Step 2 - Control Loop Example

UCA: Command to open full-load valve by one increment is not given
Bridge between STPA Step 2 and Step 1 - Analyzing Subsystems

Original Hierarchical Control Structure

Hierarchical Control Structure of «intelligent actuator»

Full-load valve controller

Level regulation with full-load valve

Scenarios (Complete Set)

EXEMPLARY ILLUSTRATION, WORK IN PROGRESS, © BY ZHAW, MARTIN REJZEK, 2014
Bridge between STPA Step 2 and Step 1 - Analyzing Subsystems

Original Hierarchical Control Structure

STPA Step 1 → STPA Step 2

Controller

Subsystem

Controlled Process

Same approach for any definition of a “subsystem”

Examples:
- reused system
- system developed by third-party

Hierarchical Control Structure of a Subsystem

STPA Step 1 → STPA Step 2

Scenarios (Subsystem)

Scenarios (Complete Set)
STPA Step 2 - Generic Control Loop

Unsafe Control Action (UCA)

Other Controller(s)

Controller

Control Action

Feedback Channel

Actuator(s)

Sensor(s)

Other Controller(s)

Process

Unwanted Process Reaction (UPR)
STPA Step 2 - Scenario Organization

Unwanted Process Reaction (UPR)

Unsafe Control Action (UCA)
Conclusion

• Process to «transform» an I&C system specification into a hierarchical control structure
  – Found a systematic and reproducible process
  – Generation of HCS could be partially automated
  – Based on system specification with (little) additions

• Formalization of the STPA step 2 questions:
  – «Scenarios resulting in {CA} {Keyword}»
  – «Scenarios leading to {UPR}»

• Explicit process to handle «subsystems»
  – Prioritization possible at each level
  – Organization of the scenarios in a generic fault tree
  – Link to results from other hazard analyses (FTA, ETA, …)
Current Activities

• Advance the case study
  – Complete STPA step 1 for all control actions
  – Continue with STPA step 2 for selected UCA’s

• Advance investigation of “blended-approach”
  – With respect to systems and subsystems
  – With respect to different analysis methods
Certain things can only be seen from a different standpoint!
Anamorphosis
Contact:

Dipl. el. Ing. FH Martin Rejzek
E-mail: martin.rejzek@zhaw.ch
http://www.iamp.zhaw.ch/sks