

STPA analysis of Sample Analysis

Just an example of analysis

Begin date: 09/06/2021 14:15:44

Report created at: 03/04/2023 13:58:12

Step One - Purpose of the Analysis

Goals

G-1: Goal One

Assumptions

A-1: Assumption One

Losses

L-1: Loss One

L-2: Loss Two

System-level Hazards

H-1: Hazard One [L-1]

H-2: Hazard Two [L-1] [L-2]

H-3: TEST [L-1]

System-level Safety Constraints

SSC-1: Safety Constraint One [H-1]

SSC-2: Safety Constraint Two [H-2]

Step Two - Control Structure

Controller Controller

Responsibilities:

R-1: asdasdsadsa 33333333. [SSC-2]

R-2: dddd. [SSC-1]

Outgoing connections

Controller -> Actuator

Control actions: cmd_01, cmd_02

Controller -> Higher-level Controller

Incoming connections

Sensor -> Controller

Feedbacks (variables and values):

feed_sensor (feed_sensor_01, feed_sensor_02)

External System -> Controller

Feedbacks (variables and values):

ext_info (ext_info_01, ext_info_02)

Higher-level Controller -> Controller

Controller Higher-level Controller

Responsibilities:

Outgoing connections

Higher-level Controller -> Controller

Control actions: cmd_ctrl_02, cmd_ctrl_01

Higher-level Controller -> Controlled Process

Control actions: cmd_hlc_01, cmd_hlc_02

Incoming connections

Controller -> Higher-level Controller

Feedbacks (variables and values):

feed_ctrl (feed_ctrl_01, feed_ctrl_02)

Controlled Process -> Higher-level Controller

Feedbacks (variables and values):

feed_cp (feed_cp_01, feed_cp_02)

TEST-VAR ()

Controller TEST CONTROLLER (external of analysis)

Responsibilities:

Outgoing connections

Incoming connections

Sensor -> TEST CONTROLLER

Actuator Actuator

Outgoing connections

Actuator -> Controlled Process

Incoming connections

Controller -> Actuator

Sensor Sensor

Outgoing connections

Sensor -> Controller

Sensor -> TEST CONTROLLER

Incoming connections

Controlled Process -> Sensor

External System External System

Outgoing connections

External System -> Controller

Incoming connections

Controlled Process Controlled Process

Outgoing connections

Controlled Process -> Sensor

Controlled Process -> Higher-level Controller

Incoming connections

Actuator -> Controlled Process

Higher-level Controller -> Controlled Process

Input: input_01, input_02

Output: output_01, output_02

Environmental Disturbances: Environmental Disturbances

Step Three - Unsafe Control Actions

Unsafe Control Actions (UCA) and Safety Constraints (SC)

Recommendation 1: (Controller: Controller - Control Action: cmd_01)

UCA-1: Controller provided in wrong order cmd_01 in any context. [H-1]

Description:

SC-1: Controller must not provide in wrong order cmd_01 in any context.

Recommendation 2: (Controller: Controller - Control Action: cmd_01)

UCA-2: Controller stopped too soon cmd_01 when feed_sensor is feed_sensor_01, ext_info is ext_info_02. [H-3]

Description: HAZard in some situation.....

SC-2: Controller must not provide to soon cmd_01 when feed_sensor is feed_sensor_01, ext_info is ext_info_02.

Recommendation 3: (Controller: Controller - Control Action: cmd_01)

UCA-3: Controller not provided cmd_01 when feed_sensor is feed_sensor_02, ext_info is ext_info_01. [H-2]

Description:

SC-3: Controller must provide cmd_01 when feed_sensor is feed_sensor_02, ext_info is ext_info_01.

Recommendation 4: (Controller: Controller - Control Action: cmd_01)

UCA-4: Controller provided cmd_01 when feed_sensor is feed_sensor_02. [H-3][H-2]

Description:

SC-4: Controller must not provide cmd_01 when feed_sensor is feed_sensor_02.

Recommendation 5: (Controller: Controller - Control Action: cmd_01)

UCA-5: Controller provided cmd_01 in any context. [H-3][H-2]

Description:

SC-5: Controller must not provide cmd_01 in any context.

Recommendation 6: (Controller: Controller - Control Action: cmd_01)

UCA-6: Controller provided in wrong order cmd_01 when VAR_ERR is VAL_ERR. [H-2]

Description:

SC-6: Controller must not provide in wrong order cmd_01 when VAR_ERR is VAL_ERR.

Recommendation 7: (Controller: Higher-level Controller - Control Action: cmd_ctrl_01)

UCA-7: Higher-level Controller provided in wrong order cmd_ctrl_01 when feed_ctrl is feed_ctrl_01, feed_cp is feed_cp_01. [H-2]

Description:

SC-7: Higher-level Controller must not provide in wrong order cmd_ctrl_01 when feed_ctrl is feed_ctrl_01, feed_cp is feed_cp_01.

Step Four - Loss Scenarios and Recommendations

R-1 (Higher-level Controller Algorithm in Higher-level Controller): UCA-7

Cause: An incorrect Higher-level Controller Algorithm was designed.

Recommendation: The Higher-level Controller Algorithm must be revised and tested after each change to minimize errors.

Mechanism:

R-2 (Sensor -> Controller): UCA-1

Cause: Temporary obstruction not allow the reading of the Controlled Process by the Sensor.

Recommendation: Alternative sensor to read the Controlled Process should be considered.

Mechanism:

R-3 (Controlled Process Input -> Controlled Process): UCA-3

Cause: Controlled Process Input (input_01 or input_02) is wrong.

Recommendation: The correct Controlled Process must be chosen according to Controlled Process Input.

Mechanism:

Link Report

Actuator -> Controlled Process

Controlled Process -> Sensor