STPA analysis of Sample Analysis

Just an example of analisys

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

Report created at: 05/04/2023 17:16:25

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: Hazard Three [L-1]

Systel-level Safety Constraints

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

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

Step Two - Control Structure

Controller controller A

Responsibilities:

R-1: Responsability One. [SSC-1]

R-2: Responsability Two. [SSC-2]

Outgoing connections

controller A -> actuator

Control actions: cmd_01, cmd_02

controller A -> higher-level controller

Incoming connections

sensor -> controller A

Feedbacks (variables and values):

feed_sensor (feed_sensor_01, feed_sensor_02)

external system -> controller A

Feedbacks (variables and values):

ext_info (ext_info_01, ext_info_02)

higher-level controller -> controller A

Controller higher-level controller

Responsibilities:

Outgoing connections

higher-level controller -> controller A

Control actions: cmd_ctrl_02, cmd_ctrl_01

higher-level controller -> controlled process

Control actions: cmd_hlc_01, cmd_hlc_02

Incoming connections

controller A -> 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 (a, b)

Controller controller B (external of analysis)

Responsibilities:

Outgoing connections

controller B -> external system

Incoming connections

sensor -> controller B

Actuator actuator

Outgoing connections

actuator -> controlled process

Incoming connections

controller A -> actuator

Sensor sensor

Outgoing connections

sensor -> controller A

sensor -> controller B

Incoming connections

controlled process -> sensor

External System external system

Outgoing connections

   external system -> controller A

Incoming connections

   controller B -> external system

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 A - Control Action: cmd_01)

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

   Description:

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

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

UCA-2: controller A 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 A must not provide to soon cmd_01 when feed_sensor is feed_sensor_01, ext_info is ext_info_02.

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

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

Description:

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

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

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

Description:

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

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

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

Description:

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

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

UCA-6: controller A provided in wrong order cmd_01 when ext_info is ext_info_01. [H-1]

Description:

SC-6: controller A must not provide in wrong order cmd_01 when ext_info is ext_info_01.

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 (controller A Process Model in controller A): UCA-1

Type: Unsafe controller behavior

Cause: Current state of controller A Process Model is wrong.

Recommendation: The process model of controller A must represent the controlled process.

Mechanism:

Link with energy

actuator -> controlled process

controlled process -> sensor

Show control structure images

No control structure images found.