

STPA for Troubleshooting Assistant

Step 1 - Losses and Hazards

Identify losses, accidents, and hazards for the system.

System-level accidents (Undesired events that result in losses)

L	Losses
L-1	Injury to worker
L-2	Damage to the machine
L-3	Excessively costly troubleshooting
L-4	Production stand-still

Hazards (System states that lead to accidents)

H	Hazard	Causes
H-1	Machine is used inappropriately	L-1, L-2, L-4
H-2	Part/mould is redesigned, but defects persist	L-3, L-4
H-3	Troubleshooting is ineffective	L-4

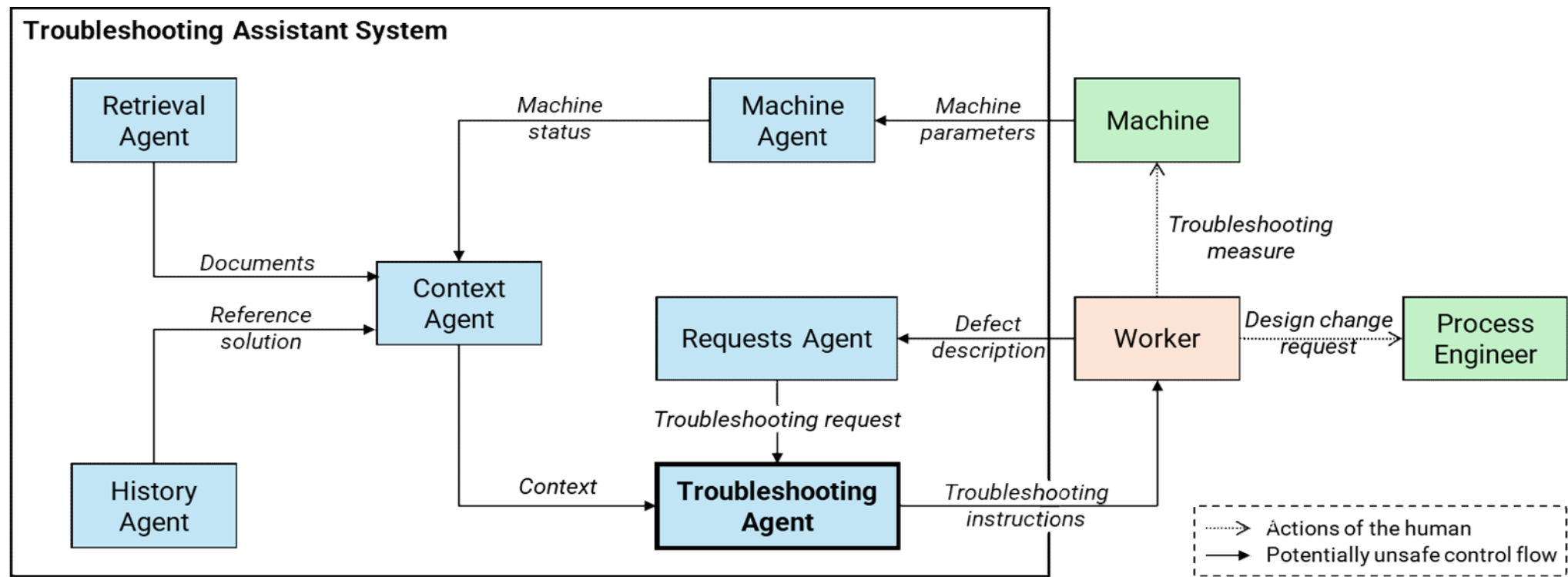
System-level Safety Constraints

SLSC	Safety Constraint	Hazards
SLSC-1	The machine must be used appropriately	H-1
SLSC-2	The part/mould should be redesigned to eliminate all defects	H-2
SLSC-3	The troubleshooting should resolve the issues	H-3

STPA for Troubleshooting Assistant

Step 2 - Control structure

Construct the control structure.



Task descriptions of components

Component	Task
Requests Agent	Receive defect description and reformulate it into a troubleshooting request
Machine Agent	Receive machine parameters from the running machine and create a status description
Retrieval Agent	Retrieve applicable documents from a database and create a summary document
History Agent	Retrieve similar processes from the past from a database and create a reference solution
Context Agent	Build a context for the troubleshooting request based on the current machine status, static documents, and past processes
Troubleshooting Agent	Generate troubleshooting instructions based on a request and a context

STPA for Troubleshooting Assistant

Step 3 - Unsafe control actions and safety constraints

Identify unsafe control actions (UCAs) and safety constraints (SCs) for each component.

Safety relevant

Hazards		Unsafe control actions types		Unsafe agent actions types	
H Hazards		Unsafe control action types		Unsafe agent action types	
1 Machine is used inappropriately		Not providing causes hazard		Message is incorrect	
2 Part/mould is redesigned, but defects persist		Providing causes hazard		Message is missing critical information	
3 Troubleshooting is ineffective		Incorrect timing/order		Message has incorrect order	
		Stopped too soon/applied too long		Message takes too long	
Unsafe control actions of components					
UCA	Component	Control action	Type	Description	Causes
	1 Worker	Troubleshooting measure	Not providing causes hazard	Worker does not attempt troubleshooting even though defects are observed	H-3
	2 Worker	Troubleshooting measure	Providing causes hazard	Worker attempts troubleshooting measures that are not appropriate for the machine type	H-1
	3 Worker	Troubleshooting measure	Providing causes hazard	Worker sets machine parameters to values that exceed the machine's limits	H-1
	4 Worker	Troubleshooting measure	Providing causes hazard	Worker applies ineffective troubleshooting measures	H-3
	5 Worker	Troubleshooting measure	Incorrect timing/order	Worker attempts measures in the wrong order	H-3
	6 Worker	Design change request	Not providing causes hazard	Worker attempts other measures when only a design change is useful	H-3
	7 Worker	Design change request	Providing causes hazard	Worker requests part/mould design change when parameter change would have been sufficient	H-2
	8 Troubleshooting Agent	Troubleshooting instructions	Message is missing critical information	No troubleshooting instructions provided	UCA-1
	9 Troubleshooting Agent	Troubleshooting instructions	Message is incorrect	Instructions recommend parameter change when only a design change would be usefull	UCA-6
	10 Troubleshooting Agent	Troubleshooting instructions	Message is incorrect	Instructions are not appropriate for the machine type	UCA-2
	11 Troubleshooting Agent	Troubleshooting instructions	Message is incorrect	Instructions contain machine parameters that exceed the machine's limits	UCA-3
	12 Troubleshooting Agent	Troubleshooting instructions	Message is missing critical information	Provided instructions are ineffective	UCA-4
	13 Troubleshooting Agent	Troubleshooting instructions	Message has incorrect order	Instructions recommend measures in the wrong order	UCA-5
	14 Troubleshooting Agent	Troubleshooting instructions	Message is incorrect	Instructions recommend design change when parameter change would have been sufficient	UCA-7
	15 Requests Agent	Troubleshooting request	Message is missing critical information	Request does not contain all information of the defect description	UCA-8, UCA-9, UCA-12, UCA-13, UCA-14
	16 Requests Agent	Troubleshooting request	Message is incorrect	Request contains additional information not in the defect description	UCA-8, UCA-9, UCA-12, UCA-13, UCA-14
	17 Worker	Defect description	Not providing causes hazard	Worker omits necessary details from the defect description	UCA-15
	18 Worker	Defect description	Providing causes hazard	Worker uses incorrect terminology in defect description	UCA-15, UCA-16
	19 Context Agent	Context	Message is missing critical information	Context Agent omits necessary details about machine parameters from the context description	UCA-9, UCA-10, UCA-11, UCA-12, UCA-13, UCA-14
	20 Context Agent	Context	Message is missing critical information	Context Agent omits necessary details about static documents from the context description	UCA-9, UCA-10, UCA-11, UCA-12, UCA-13, UCA-14
	21 Context Agent	Context	Message is missing critical information	Context Agent omits necessary details about past processes from the context description	UCA-9, UCA-12, UCA-13, UCA-14
	22 Context Agent	Context	Message is incorrect	Context Agent adds incorrect details about machine parameters to the context description	UCA-9, UCA-10, UCA-11, UCA-12, UCA-13, UCA-14
	23 Context Agent	Context	Message is incorrect	Context Agent adds incorrect details about static documents to the context description	UCA-9, UCA-10, UCA-11, UCA-12, UCA-13, UCA-14
	24 Context Agent	Context	Message is incorrect	Context Agent adds incorrect details about past processes to the context description	UCA-9, UCA-12, UCA-13, UCA-14
	25 Context Agent	Context	Message is incorrect	Context Agent adds irrelevant details about static documents to the context description	UCA-9, UCA-10, UCA-11, UCA-12, UCA-13, UCA-14
	26 Context Agent	Context	Message is incorrect	Context Agent adds irrelevant details about past processes to the context description	UCA-9, UCA-10, UCA-11, UCA-12, UCA-13, UCA-15
	27 Machine Agent	Machine status	Message is missing critical information	Machine Agent omits one or multiple machine parameters from the machine status	UCA-19
	28 Machine Agent	Machine status	Message is incorrect	Machine Agent provides incorrect machine status	UCA-22
	29 Machine	Machine parameters	Message is incorrect	Machine provides incorrect parameter values	UCA-28
	30 Machine	Machine parameters	Message is incorrect	Machine provides incorrect parameters	UCA-28
	31 Retrieval Agent	Documents	Message is missing critical information	Documents summary do not contain information that should be part of the context	UCA-20
	32 Retrieval Agent	Documents	Message is incorrect	Documents summary contains incorrect information	UCA-23
	33 Retrieval Agent	Documents	Message is incorrect	Documents summary contains too much irrelevant information	UCA-25
	34 History Agent	Reference solution	Message is missing critical information	Reference solution is not based on a similar process from the past	UCA-21
	35 History Agent	Reference solution	Message is incorrect	Reference solution contains incorrect information	UCA-24
	36 History Agent	Reference solution	Message is incorrect	Reference solutions contains too much irrelevant information	UCA-26

STPA for Troubleshooting Assistant

Step 3 - Unsafe control actions and safety constraints

Identify unsafe control actions (UCAs) and safety constraints (SCs) for each component.

Safety relevant

Hazards		Unsafe control actions types		Unsafe agent actions types	
H	Hazards	Unsafe control action types		Unsafe agent action types	
1	Machine is used inappropriately	Not providing causes hazard		Message is incorrect	
2	Part/mould is redesigned, but defects persist	Providing causes hazard		Message is missing critical information	
3	Troubleshooting is ineffective	Incorrect timing/order		Message has incorrect order	
		Stopped too soon/applied too long		Message takes too long	
Safety constraints of components					
SC	Component	Control action	Type	Description	UCA
1	Worker	Troubleshooting measure	Not providing causes hazard	Worker must attempt troubleshooting when defects are observed	UCA-1
2	Worker	Troubleshooting measure	Providing causes hazard	Worker must only attempt troubleshooting measures appropriate for the machine type	UCA-2
3	Worker	Troubleshooting measure	Providing causes hazard	Worker must only set machine parameters within their limits	UCA-3
4	Worker	Troubleshooting measure	Providing causes hazard	Worker must only apply effective troubleshooting measures	UCA-4
5	Worker	Troubleshooting measure	Incorrect timing/order	Worker must keep the order of measures	UCA-5
6	Worker	Design change request	Not providing causes hazard	Worker must proceed with design changes when only their are usefull	UCA-6
7	Worker	Design change request	Providing causes hazard	Worker must only request design changes when parameter changes wouldn't be sufficient	UCA-7
8	Troubleshooting Agent	Troubleshooting instructions	Message is missing critical information	Troubleshooting Agent must always provide troubleshooting instructions	UCA-8
9	Troubleshooting Agent	Troubleshooting instructions	Message is incorrect	Troubleshooting Agent must recommend design changes when they are necessary	UCA-9
10	Troubleshooting Agent	Troubleshooting instructions	Message is incorrect	Troubleshooting Agent must only give instructions appropriate for the machine type	UCA-10
11	Troubleshooting Agent	Troubleshooting instructions	Message is incorrect	Troubleshooting Agent must only give parameter instrucionts within the machine's limits	UCA-11
12	Troubleshooting Agent	Troubleshooting instructions	Message is missing critical information	Troubleshooting Agent must only provide effective instructions	UCA-12
13	Troubleshooting Agent	Troubleshooting instructions	Message has incorrect order	Troubleshooting Agent must recommend instructions in the correct order	UCA-13
14	Troubleshooting Agent	Troubleshooting instructions	Message is incorrect	Troubleshooting Agent must recommend parameter changes when they would be sufficient	UCA-14
15	Requests Agent	Troubleshooting request	Message is missing critical information	Request Agent must include all information from the defect description in the request	UCA-15
16	Requests Agent	Troubleshooting request	Message is incorrect	Request Agent must only include information from the defect description in the request	UCA-16
17	Worker	Defect description	Not providing causes hazard	Worker must give the full defect description	UCA-17
18	Worker	Defect description	Providing causes hazard	Worker must use the correct defect description	UCA-18
19	Context Agent	Context	Message is missing critical information	Context Agent must include all necessary details about machine parameters in the context description	UCA-19
20	Context Agent	Context	Message is missing critical information	Context Agent must include all necessary details about static documents in the context description	UCA-20
21	Context Agent	Context	Message is missing critical information	Context Agent must include all necessary details about past processes in the context description	UCA-21
22	Context Agent	Context	Message is incorrect	Context Agent must not add incorrect details about machine parameters to the context description	UCA-22
23	Context Agent	Context	Message is incorrect	Context Agent must not add incorrect details about static documents to the context description	UCA-23
24	Context Agent	Context	Message is incorrect	Context Agent must not add incorrect details about past processes to the context description	UCA-24
25	Context Agent	Context	Message is incorrect	Context Agent must not add irrelevant details about static documents to the context description	UCA-25
26	Context Agent	Context	Message is incorrect	Context Agent must not add irrelevant details about past processes to the context description	UCA-26
27	Machine Agent	Machine status	Message is missing critical information	Machine Agent must include all machine parameters in the machine status	UCA-27
28	Machine Agent	Machine status	Message is incorrect	Machine Agent must only provide the correct machine status	UCA-28
29	Machine	Machine parameters	Message is incorrect	Machine must only provide correct parameter values	UCA-29
30	Machine	Machine parameters	Message is incorrect	Machine must always provide correct parameters	UCA-30
31	Retrieval Agent	Documents	Message is missing critical information	Documents summary must contain all relevant information	UCA-31
32	Retrieval Agent	Documents	Message is incorrect	Documents summary must only contain correct information	UCA-32
33	Retrieval Agent	Documents	Message is incorrect	Documents summary must only contain relevant information	UCA-33
34	History Agent	Reference solution	Message is missing critical information	Reference solution must be based on a similar process	UCA-34
35	History Agent	Reference solution	Message is incorrect	Reference solution must only contain correct information	UCA-35
36	History Agent	Reference solution	Message is incorrect	Reference solution must only contain relevant information	UCA-36

STPA for Troubleshooting Assistant

Step 4 - Causal factors

Identify causal factors (CFs).

Causal factors of hazardous actions

CF	Component	Source	Description	SC
	Context Agent	Inadequate control algorithm	Context request is processed incorrectly	SC-19, SC-20, SC-21
	Context Agent	Control input	Context Agent recieved incorrect context request	SC-19, SC-20, SC-21
	Context Agent	Sensor failure	Context Agent recieved incorrect data	SC-19, SC-20, SC-21, SC-22, SC-23, SC-24
	Context Agent	Inadequate control algorithm	Recieved data is processed incorrectly	SC-19, SC-20, SC-21, SC-22, SC-23, SC-24
1	Troubleshooting Agent	Control input	Received troubleshooting request without defect descriptions	SC-8
2	Troubleshooting Agent	Sensor failure	Received context without suggestions for necessary design changes	SC-9
3	Troubleshooting Agent	Inadequate control algorithm	Prompt discouraging design changes to heavily	SC-9
4	Troubleshooting Agent	Sensor failure	Received incomplete context information	SC-8, SC-9, SC-10, SC-11, SC-12, SC-13, SC-14
5	Troubleshooting Agent	Inadequate control algorithm	LLM hallucinates incorrect machine type	SC-10
6	Troubleshooting Agent	Sensor failure	Received context with incorrect info about machine type	SC-10
7	Troubleshooting Agent	Sensor failure	Received context with instructions only suitable for another machine type	SC-10
8	Troubleshooting Agent	Inadequate control algorithm	LLM hallucinates instructions unsuitable for the machine type	SC-10
9	Troubleshooting Agent	Sensor failure	Received context with incorrect machine parameter limits	SC-11
10	Troubleshooting Agent	Sensor failure	Received context with hazardous machine parameter value suggestions	SC-11
11	Troubleshooting Agent	Inadequate control algorithm	LLM hallucinates hazardous machine parameter values despite context	SC-11
12	Troubleshooting Agent	Sensor failure	Received ineffective troubleshooting instructions in context	SC-12
13	Troubleshooting Agent	Inadequate control algorithm	LLM hallucinates ineffective instructions	SC-12
14	Troubleshooting Agent	Inadequate control algorithm	LLM excludes effective/relevant instructions	SC-12
15	Troubleshooting Agent	Inadequate control algorithm	LLM missaranges troubleshooting instructions	SC-13
16	Troubleshooting Agent	Sensor failure	Received missaranged troubleshooting instructions	SC-13
17	Troubleshooting Agent	Inadequate control algorithm	LLM hallucinates effective design changes	SC-14
18	Troubleshooting Agent	Sensor failure	Received no sufficient parameter change suggestions in context	SC-14
19	Requests Agent	Inadequate control algorithm	LLM excludes defect symptoms from defect description when creating troubleshooting request	SC-15
20	Requests Agent	Inadequate control algorithm	LLM changes wording for defect symptom so that it no longer covers the actual defect description	SC-15
21	Requests Agent	Inadequate control algorithm	LLM hallucinates defect symptom not in defect description	SC-16
22	Context Agent	Inadequate control algorithm	LLM excludes machine parameters from context description	SC-19
23	Context Agent	Sensor failure	Received incomplete machine status	SC-19
24	Context Agent	Inadequate control algorithm	LLM excludes details from document summary from context description	SC-20
25	Context Agent	Sensor failure	Received incomplete document summary	SC-20
26	Context Agent	Inadequate control algorithm	LLM excludes details from reference solution from context description	SC-21
27	Context Agent	Sensor failure	Received incomplete reference solution	SC-21
28	Context Agent	Inadequate control algorithm	LLM hallucinates incorrect machine parameters for context description	SC-22
29	Context Agent	Sensor failure	Recieved incorrect machine parameters	SC-22
30	Context Agent	Inadequate control algorithm	LLM adds hallucinated incorrect document summary details to the context description	SC-23
31	Context Agent	Sensor failure	Recieved incorrect document summary	SC-23
32	Context Agent	Inadequate control algorithm	LLM adds hallucinated incorrect reference solution details to the context description	SC-24
33	Context Agent	Sensor failure	Recieved incorrect reference solution	SC-24
34	Context Agent	Inadequate control algorithm	LLM changes wording of machine parameters for the context description	SC-19, SC-22
35	Context Agent	Inadequate control algorithm	LLM changes wording of details from the document summary	SC-19, SC-22
36	Context Agent	Inadequate control algorithm	LLM changes wording of details from the reference solution irrelevant docs + example	SC-19, SC-22
37	Machine Agent	Inadequate control algorithm	LLM excludes machine parameters from the machine status	SC-27
38	Machine Agent	Sensor failure	Recieved inomplete machine parameter list	SC-27
39	Machine Agent	Inadequate control algorithm	LLM hallucinates incorrect parameter values	SC-28
40	Machine Agent	Sensor failure	Recieved incorrect machine parameters	SC-28
41	Retrieval Agent	Inadequate control algorithm	LLM excludes relevant information from the document chunks in the document summary	SC-31
42	Retrieval Agent		Retrieved incomplete list of document chunks	SC-31
43	Retrieval Agent	Inadequate control algorithm	LLM changes wording of relevant information in the document chunks	SC-31, SC-32
44	Retrieval Agent	Inadequate control algorithm	LLM hallucinates incorrect information	SC-32
45	Retrieval Agent		Retrieved document chunks contain incorrect information	SC-32
46	Retrieval Agent	Inadequate control algorithm	LLM hallucinates irrelevant information	SC-33
47	Retrieval Agent		Retrieved document chunks contain irrelevant information	SC-33
48	History Agent	Inadequate control algorithm	LLM excludes relevant information from similar processes in the reference solution	SC-34
49	History Agent		Retrieved incomplete list of similar processes	SC-34
50	History Agent	Inadequate control algorithm	LLM changes wording of relevant information from the list of similar processes	SC-34, SC-35
51	History Agent	Inadequate control algorithm	LLM hallucinates incorrect information	SC-35
52	History Agent		Retrieved list of similar processes contains incorrect information	SC-35
53	History Agent	Inadequate control algorithm	LLM hallucinates irrelevant information	SC-36
54	History Agent		Retrieved list of similar processes contains irrelevant information	SC-36

GSN for Troubleshooting Assistant

Goal Structuring Notation

