Hazard scenarios simulated by fault-injection and the observed system behavior

Potential Causal Factor	Injected Fault			No. Activated/ Injected	Observed Behavior (Hazard)	No.
	Location Target Function: Variables	Value	Type			
Incorrect console inputs	network_process u.delx, udely, or udelz u.R_l or u.R_r	Out of range	StuckAt	20/20	Homing: No impact Pedal Down: IK-failure, small jumps, No movement, No E-STOP or E-STOP, depending on the arms configuration (H3)	1
			Intermittent (for 10, 100, 500 packets)	40/40	Homing: No impact Pedal Down: IK-failure, No movement or small jumps, No E-STOP or E-STOP depending on the arms configuration (H1-2, H3)	2
	network_process surgeon_mode	0	StuckAt	5/5	Homing: No impact Pedal Down: Does not start movement (H3)	3
		1	StuckAt	0/5	Homing: No impact	4
		0/1	Periodic Flipping (every 30, 100, 300, or 1000 cycles)	15/15	Pedal Down: Movement stops or small jumps (H1-2, H3) PLC stops at very high flipping rate. (H3)	5
Faulty control algorithm	r2_inv_kin jpos_d	0,100, 1000	StuckAt	10/10	After homing, E-STOP (overdrive_detect)	6
	invMechCableCoupling mpos_d	0, 100,000	StuckAt	10/10	E-STOP (overdrive_detect)	7
			Periodic Flipping			8
	mpos_PD_control joint>tau_d	0, 1, -1, 100,000 -100,000	StuckAt	5/5	Does not move when StuckAt 0 (H3), otherwise E-STOP	9
			Periodic Flipping	5/5	No impact when StuckAt 0, otherwise E-STOP	10
	TorqueToDAC joint[i].current_cmd	-1000	StuckAt	1/1	Abrupt jump, causing cable break on left and right arms (H1-2, H2, H3)	11
	stateEstimate mpos	0, -1	StuckAt or Periodic Flipping	10/10	E-STOP (overdrive_detect)	12
	stateEstimate mvel		StuckAt	5/5	Homing: Unintended rotation, E-STOP (H2)	13

			Periodic Flipping	3/3	Homing: Unintended tool movement, collision to the floor (H1-2, H2, H3)	14
					Pedal Down: No impact	15
	fwdCableCoupling joint[i].jpos	0,100, 1000	StuckAt	8/10	IK-fail and E-STOP when very large number injected (overdrive_detect)	16
	fwdCableCoupling joint[i].jvel			0/10	No impact	17
	r2_fwd_kin pos.x, pos.y, pos.z,	0, 1000 100,0000	StuckAt	1/5	Homing: No Impact, Pedal Down: E-STOP (overdrive_detect)	18
	r2_fwd_kin ori_R			10/10	Homing: No Impact Pedal Down: E-STOP, or IK-fail with no E-STOP	19
	stateMachine rlDesired	0	StuckAt	16/16	Homing: Does not start, software assumes hardware is in E-STOP but it is in Init After Homing: movement stops because software stops sending foot pedal to hardware causing it to move to Pedal up state (H3)	20
		1			Homing: Starts homing but E-STOP happens, After homing: movement stops because software stops sending foot pedal to hardware causing it to move to Pedal up state (H3)	21
		2			Homing: Does not start, software assumes hardware is in E-STOP but it is in Init After Homing: movement stops because software goes to pedal up, hardware remains in pedal down (H3)	22
		3			Homing: Does not start, software assumes hardware is in E-STOP but it is in Init (H3) After Homing: No impact	23

Faulty USB communication	getUSBPackets USBBoards.activeAtStart	0	StuckAt	10/10	Homing: Stopped, does not start moving After Homing: Hardware E-STOP happened but not reported, but no software E-STOP, software keeps running, watchdog sent but not received by PLC (H3)	24
		1 >2		10/10	Homing: Stopped, does not start moving	25
	getUSBPackets USBBoards.boards[i]	2	StuckAt	10/10	After Homing: Hardware E-STOP reported (by reading through one pin), but no software E-STOP, software keeps running, watchdog sent but not received by PLC (H3)	26
	getUSBPackets buffer	Random	StuckAt	10/10	Homing: No impact After Homing: Hardware and software E-STOP (overdrive_detect)	27
	getUSBPackets mech>inputs	0	StuckAt	12/12	Homing: Does not move, software assumes hardware is in E-STOP (H3) After Homing: E-STOP, software assumes hardware is in E-STOP so goes to E-STOP and stops sending watchdog, causing hardware to really go to E-STOP (H3)	28
			Periodic Flipping (every 30, 100, 300, or 1000 cycles)	10/10	Homing: Repeats the homing process over and over again (H2, H3). After Homing: Hardware completely stops (30, 100) or brakes are applied repeatedly (1000, 3000) (H2, H3)	29
	putUSBPackets USBBoards.activeAtStart	<= 0	StuckAt	20/20	Homing: If early during homing, Raven software (PLC state stuck at 0) keeps running, but homing not started because it is not writing anything to the boards. If during checking the joint limits, IK fails leading to Software E-Stop detected and triggered but not reported because the software doesn't get the Hardware E-STOP confirmation in the state machine. Hardware E-stop	30

					because no watchdog is sent due to software E-stop. After Homing: If in the middle of packet processing, Hardware E-Stop happened but not reported and no software E-stop, software keeps running with no movements (H3)	
		1		10/10	Homing: Raven software (PLC state stuck at 0) keeps running, but homing not started because it is not writing anything to the boards. After Homing: Hardware E-STOP reported (through reading one pin), but no software E-stop, software keeps running (H3)	31
		>2		10/10	Homing: If early in the homing process, Raven process crashed after checking for USB boards (SegFault) After Homing: Raven process keeps reporting PLC state, but it crashed either after checking for USB boards or in the middle of packet processing (Segfault) (H3)	32
	putUSBPackets USBBoards.boards[i]	2	StuckAt	10/10	Homing: If early during homing, bzlups100us going on for a while after checking USB boars during init process, but then robot runs with no problem If later during homing, many bzlups100us going on for a while, then software and hardware E-stop due to IK failure. After Homing: bzlups100us going on continuously and Hardware E-stop happened but not reported and no software E-Stop (H3)	33

	putUSBPackets joint[i].current_cmd	Random	StuckAt	3/5	Homing: No Impact. After Homing: Software E-STOP and very abrupt jump (H1-2, H2, H3)	34
	putUSBPackets mech>outputs	0, 1, 2	StuckAt	16/16	Homing: Does not start homing, hardware stuck at E-STOP (H3) After Homing: Hardware goes to E-STOP and stops the movement	35
		3			After Homing: No impact	36
Missing/ incorrect output from software to PLC	updateAtmelOutputs surgeon_mode	0	StuckAt	10/10	Homing: No impact After Homing: Hardware goes to E-STOP after being in Pedal UP for a while	37
		1			After Homing: Software and hardware in Pedal Down already, don’t receive packets from packet gen	38
	updateAtmelOutputs runlevel	0	StuckAt	20/20	Homing: Does not start homing, hardware stuck at E-STOP (H3) After Homing, Hardware goes to Pedal UP because software stops sending foot pedal signal	39
		1			Homing: No impact After Homing: Hardware goes to Pedal UP because software stops sending foot pedal signal (H3)	40
		2			No impact	41
		3				42
	updateAtmelOutputs initialized	0	StuckAt	10/10	Homing: Does not start (H3) After Homing: No impact	43
		1			Does not do homing, hardware goes to Pedal Down state. (H3) After Homing: No impact	44
Missing/ incorrect input to software from PLC	updateAtmelInputs PLCState	0, 1, 2, 3	StuckAt	5/5	No Impact, Warning Message	45