NORTHROP GRUMMAN

Using STPA to Improve Robotic Manufacturing of a Rocket Motor

Bryan Smith
Jeremy Hatch
Paul Clark
Garrett Cranney

June 2023

NORTHROP GRUMMAN

Rocket Motor Static Test

https://www.northropgrumman.com/space/propelling-space-and-defense-missions-solid-rocket-motor-expertise/

Introduction

- Rocket motor propellant
  - Solid
  - Composite
- Fanuc robots
  - User frame
- Some of the processes that are involved in production
  - Producing the propellant
  - Producing the case
  - Producing the nozzle
- Rotation

Fanuc Robots, Collaborative Welding Robot Controller (acieta.com)

https://www.northropgrumman.com/space/propelling-space-and-defense-missions-solid-rocket-motor-expertise/

STPA of Robot Propellant Cutting (Example)

STPA Step 1 – Robot Propellant Cutting

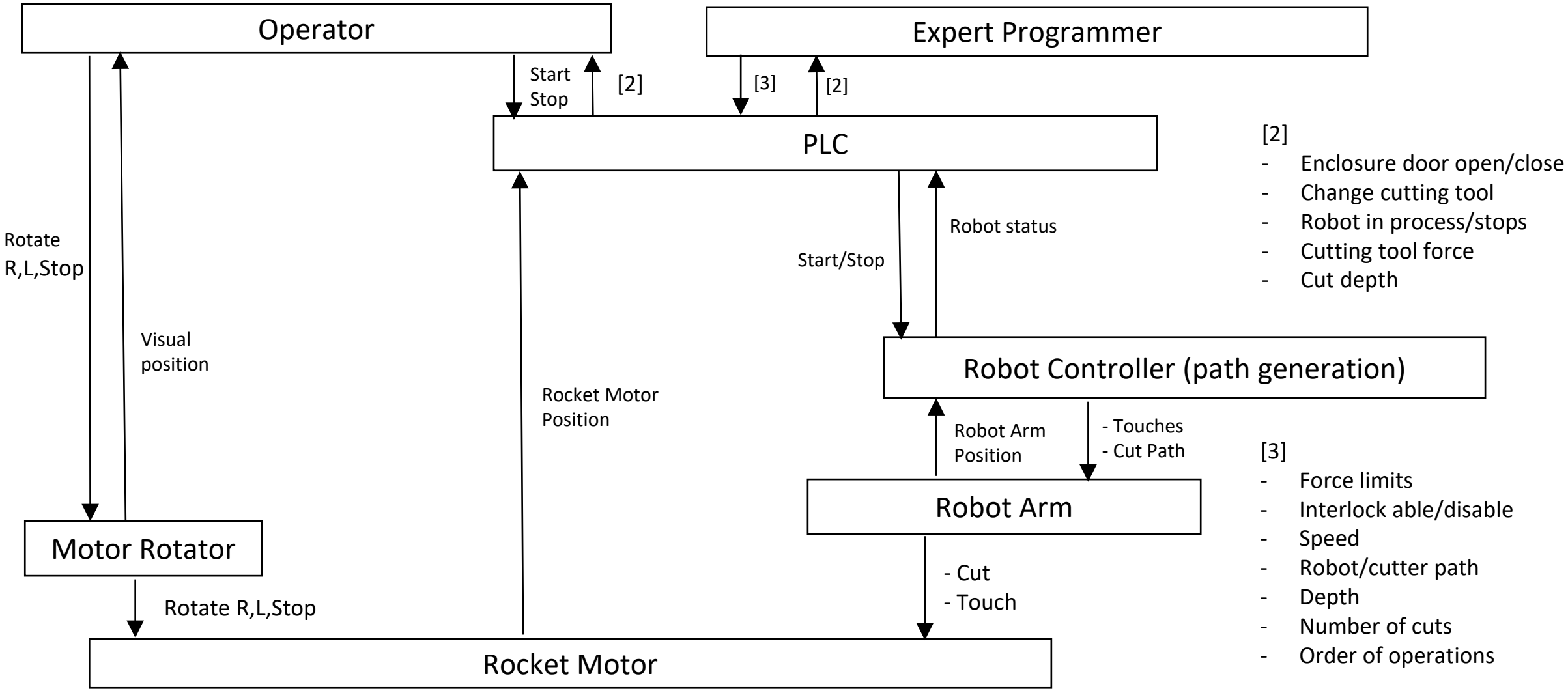
Stakeholder Losses

- L1: Human injury or loss of life
- L2: Loss of manufacturing/production capability (loss of continued production ability: robot, facility, etc.)
- L3: Damage of property (internal or external company)
- L4: Significant environmental release (possibly only minor for this application)
- L5: Loss or damage of product

System-level Hazards (Robot)

- H1: Robot makes contact with a person (directly or indirectly) [L1, L2]
- H2: Robot makes unintended contact with rocket motor (non-initiation) (e.g. zone A may have lower threshold for “damaging contact”, etc.) [L2, L3, L5, L6]
- H3: Robot creates conditions that are not suitable for segment (e.g. ignites segment, high heat, fire, sparking, etc.) [L1, L2, L3, L4, L5]
- H4: Robot damage (i.e. handling is done improperly damages robot or rocket motor) [L1, L2, L3, L5]

STPA Step 2 – Robot Propellant Cutting Control Structure (Simplified)



STPA Step 3 – Unsafe Control Actions

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
Source: Robot Control Action: Cut	UCA-R-1: Robot does not provide Cut when robot, casing, and operator are ready and in position (see note 1) [H?]	UCA-R-2: Robot does provide Cut when the cutting pass is not removing adequate material [H3, H4]	UCA-R-7: Robot provides Cut too late after operator is ready (see note 2) [H1]	UCA-R-13: Robot continues providing Cut too long after a Stop Condition* is triggered [H1]
		UCA-R-3: Robot does provide Cut when cutting tool is in a position to remove excessive propellant material (see note 3) [H3, H4]	UCA-R-8: Robot provides Cut too late after motor has rotated out of starting position [H2, H3, H4]	UCA-R-14: Robot stops providing Cut too soon before cutting blade exits the propellent (i.e. before it finishes cutting the propellent) [H3, H4]
		UCA-R-4: Robot does provide Cut when the cutting tool is in a position to cut non-propellant (e.g. case, insulation) [H2, H3, H4]	UCA-R-9: Robot provides Cut too early before the motor has rotated into starting position [H2, H3, H4]	UCA-R-15: Robot continues providing Cut beyond end point of cut path [H2, H3, H4]
		UCA-R-5: Robot does provide Cut when a person is present within range of the robot arm [H1]	UCA-R-10: Robot provides Cut too early before the operator is ready (not plausible)	
		UCA-R-6: Robot does provide Cut when a person is present in the room where propellant is cut (see note 4) [H1]	UCA-R-11: Robot provides Cut before accurate position feedback is available from position or force feedback sensors [H2, H3, H4]	
		UCA-R-12: Robot provides Cut when the Cut depth or speed is excessive (see note 5) [H3, H4]		
		UCA-R-16: Robot provides Cut when tool is not ready (not installed, damaged, dull, incorrect installation) [H3, H4]		

[1] Operator in position = operator is at station and fence is closed
[2] Operator is ready = operator has pressed green “go” button
[3] cutting too much material causes excessive strain on the cutting bit which can lead to H-3, H-4
[4] this could expose persons to harmful environment as the propellant is cut
- Stop condition = E-stop, programmed stop, …

[5] excessive depth or speed can generate heat and lead to H-?

STPA Step 3 – Unsafe Control Actions

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
Source: Operator Control Action: Rotate Motor	UCA-O-1: Operator does not provide Rotate when previous cut has completed (note 1) [H2, H3, H4]	UCA-O-6: Operator provides Rotate when the robot is cutting [H2, H3, H4]	UCA-O-12: Operator provides Rotate too early before the chip catcher has been positioned in a way that won't interfere with rotation	UCA-O-14: Operator continues providing Rotate too long after the motor reaches the correct position for cutting
	UCA-O-2: Operator does not provide Rotate when the motor is not in correct position prior to cutting [H2, H3, H4]	UCA-O-7: Operator provides Rotate when the motor is already in correct position for cutting	UCA-O-13: Operator provides Rotate too late after (or while) the next series of cuts is initiated	UCA-O-15: Operator stops rotate too soon before the motor reaches the correct position for cutting
		UCA-O-8: Operator provides Rotate when the collected chips from previous cut have not been cleared away (see note 2)		
		UCA-O-9: Operator provides Rotate when equipment is in the path of rotation		
		UCA-O-10: Operator provides Rotate when a person is in the path of rotation		
		UCA-O-11: Operator provides Rotate when chips have fallen into an area that would interfere with rotation (see note 3)		

[1] if robot cuts, operator doesn't rotate, then the robot may try to cut with the motor not in position, that would damage the motor because we cut it too deep
[2] assume the chips fall where they are supposed to be. Could also potentially affect visibility?
[3] assume the chips fall where they aren't supposed to be
[4] Assume manually rotate

STPA Step 3 – Unsafe Control Actions

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
Source: PLC stop	UCA-P-1: PLC does not provide stop when person is in range of robot.	UCA-P-3: PLC provides stop when tool is in contact with propellant.(1)	UCA-P-5: PLC provides stop too late when person is in range of robot.	
	UCA-P-2: PLC does not provide stop when operator commands stop.	UCA-P-4: PLC provides stop when arm is in path of rotation.(2)	UCA-P-5: PLC provides stop too late after robot collision with object.	
			UCA-P-6: PLC provides stop too late after robot collision with object is inevitable. (3)	

[1] Mitigate by design to prevent hazardous condition
[2] The arm is stopped in the path of the rotating propellant path
[3] Discussion based on point of no return, momentum carries the arm into the object

STPA Step 3 – Unsafe Control Actions

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early, too late, out of order	Stopped too soon, applied too long
Source: Robot Control Action: Cut	UCA-R-1: Robot does not provide Cut when robot, casing, and operator are ready and in position (see note 1) [H?]	UCA-R-2: Robot does provide Cut when the cutting pass is not removing adequate material [H3, H4]	UCA-R-7: Robot provides Cut too late after operator is ready (see note 2) [H1]	UCA-R-13: Robot continues providing Cut too long after a Stop Condition* is triggered [H1]
		UCA-R-3: Robot does provide Cut when cutting tool is in a position to remove excessive propellant material (see note 3) [H3, H4]	UCA-R-8: Robot provides Cut too late after motor has rotated out of starting position [H2, H3, H4]	UCA-R-14: Robot stops providing Cut too soon before cutting blade exits the propellent (i.e. before it finishes cutting the propellent) [H3, H4]
		UCA-R-4: Robot does provide Cut when the cutting tool is in a position to cut non-propellant (e.g. case, insulation) [H2, H3, H4]	UCA-R-9: Robot provides Cut too early before the motor has rotated into starting position [H2, H3, H4]	UCA-R-15: Robot continues providing Cut beyond end point of cut path [H2, H3, H4]
		UCA-R-5: Robot does provide Cut when a person is present within range of the robot arm [H1]	UCA-R-10: Robot provides Cut too early before the operator is ready (not plausible)	
		UCA-R-6: Robot does provide Cut when a person is present in the room where propellant is cut (see note 4) [H1]	UCA-R-11: Robot provides Cut before accurate position feedback is available from position or force feedback sensors [H2, H3, H4]	
		UCA-R-12: Robot provides Cut when the Cut depth or speed is excessive (see note 5) [H3, H4]		
		UCA-R-16: Robot provides Cut when tool is not ready (not installed, damaged, dull, incorrect installation) [H3, H4]		

[1] Operator in position = operator is at station and fence is closed
[2] Operator is ready = operator has pressed green “go” button
[3] cutting too much material causes excessive strain on the cutting bit which can lead to H-3, H-4
[4] this could expose persons to harmful environment as the propellant is cut
- Stop condition = E-stop, programmed stop, …

[5] excessive depth or speed can generate heat and lead to H-?

STPA Step 4 – Robot Propellant Cutting Scenarios

Unsafe Control Action

UCA-R-4: Robot does provide Cut when the cutting tool is in a position to cut non-propellant (e.g. case, insulation) [H2, H3, H4]

- Scenario 1
  - The robot provides a cut when the cutting tool is in a position to cut non-propellant because the operator believes the robot user frame has already been set when it has not. The operator believes the user frame has already been set previously because it is sometimes performed by another operator (ambiguous responsibility) and there is no clear indication from the robot about if or when the user frame was set (missing feedback). The result is the robot cuts in an incorrect position which will damage the rocket motor case, seal, etc.
- Solutions
  - Vision system must be designed to adjust for small movements during processing or other small adjustments
    - Flag operator and stop cut if too large of an adjustment is needed
  - Force sensor can indicate a high force
    - Must trigger a limit which stops cut (interlock)
  - Procedures
    - Training must include clear responsibility for setting the user frame and when/how to verify
    - Planning must include steps to set or verify the user frame soon before cutting operation begins

STPA Step 4 – Robot Propellant Cutting Scenarios

Unsafe Control Action

UCA-R-4: Robot does provide Cut when the cutting tool is in a position to cut non-propellant (e.g. case, insulation) [H2, H3, H4]

- Scenario 2
  - The robot provides a cut when the cutting tool is in a position to cut non-propellant because the operator believes the robot or platform has not moved since the user frame was previously set. The operator could be unaware that the robot platform has moved because the system currently does not provide any clear indication about platform movement or the actual position when the user frame was last programmed (missing feedback). Platform movement could be caused by platform slipping or other maintenance work.
- Solutions
  - Add a simple mechanical means to show the platform location when the user frame is set
  - Add a pin lock
  - Add a sensor for the pin position (high reliability/failsafe sensor)
    - The position has not moved
    - The pin is in place/installed
    - Force reteach of user frame

STPA Step 4 – Robot Propellant Cutting Scenarios

Unsafe Control Action

UCA-R-4: Robot does provide Cut when the cutting tool is in a position to cut non-propellant (e.g. case, insulation) [H2, H3, H4]

- Scenario 3
  - The robot provides a cut when the cutting tool is in a position to cut non-propellant because the operator teaches the user frame incorrectly to the robot. The operator may see that the user frame was successfully programmed even though the user frame is incorrect. The robot is designed to provide confirmation that the operation is completed, not that the operation was completed correctly (difficult to determine).
- Solutions
  - Force sensor teaches the user frame to the robot (eliminates this scenario by taking the operator out of the process)
    - Triggers limit which stops cut (interlock)
  - Establish user frame limits checks within the programing
    - Flags operator and prevents completion of teaching?
  - Robot automatically verifies the user frame before starting every operation

Reflections on Performing STPA

Applying STPA to Incomplete Design

- Robot design concept was not yet finished when STPA applied. Many decisions unknown. Multiple competing concepts existed.
- We found that the control structure was not that different between concepts.
- We identified the design features that were common for each concept and defined a baseline.
- STPA was applied to the baseline, and the STPA outputs (requirements, scenarios, and mitigations) were used to drive the design and selection of concepts
- For parts of the design that were uncertain, the UCAs/scenarios were developed using worse-case assumptions.
  - E.g., For a rotate command, assume there is no chip catcher and identify the additional UCAs/scenarios that will need to be mitigated and the additional requirements that will be needed. Those STPA results can then be used to evaluate and select from the available concepts—if there is no chip catcher, these 10 additional requirements that would need to somehow be enforced by the robot.

Insights Identified During STPA

- Robot vs. Motor perspective for System-Level Hazards – Decided Robot perspective better
- Originally thought we didn't need a chip catcher, but realized we may need one (during UCAs)
- We may need the chip catcher mounted to a stand independent of rotation (during UCAs)
- Requiring operators to manually control the rotation of the rocket engine will be much slower than PLC automation to control rotation, but we're not sure if our existing knowledge and safety requirements are adequate enough to enable that automation safely.
- Identified new UCA involving the incorrect cutting tool installation, which led to additional requirements and procedures
- Decision to pin robot platform into place with a sensor to mitigate/eliminate several STPA scenarios
- Decision to use force sensor to set the user frame rather than the operator – eliminates operator based UCA-R-4
- Question raised during UCA analysis: We don't have any abort command. Should we have an abort cmd, not just a stop cmd?
  - We've had abort (return home) before on other robots
  - How would abort work: continue and finish the cut before returning home, immediately return to home?
  - If it gets stuck today, we'd want to back up the tool to get it out. (cutting tool needs sharp cut edge for cutting and backing out). Are we giving the operator that same ability with the robotic system?

NG STPA Conclusions

- Initiating the STPA prior to completion of the robotic cell design identifies critical safety controls and allows for faster implementation of those controls.
- The STPA will continue to be updated throughout the design process, with the analysis finalized after completion of the cell design.
- STPA helped identify key safety controls that will be integrated into the robot cell design. Some examples:
  - Include a propellant chip catcher. Design the propellant chip catcher to be mounted in a manner that allows for motor rotation.
  - Further analysis of Northrop Grumman procedures and safety controls is required to determine if the PLC will operate the motor rotator, or if operators will perform the rotation.
  - If the cutter gets stuck today, we'd want to back up the tool to get it out. (cutting tool needs sharp cut edge for cutting and backing out). Are we giving the operator that same ability with the robotic system?
  - Pin the robot platform into place with an interlocked sensor.
  - Design the system such that the force sensor teaches the user frame rather than the operator – eliminates operator based UCA.
  - Identified and analyzed new functionality:
    - Should we have an abort command, not just a stop command?
    - How would abort work: continue and finish the cut before returning home, immediately return to home?
  - Implement a fail-safe method for installing the cutting tools correctly.

Northrop Grumman safety board will include consideration of STPA for the first time