What do I do now that I have read the book?

or

Application of System Theoretic Process analysis to requirements and algorithms for a thrust control malfunction protection system

An approach based on "Engineering a Safer World – Systems Thinking Applied to Safety" *Leveson (2011)*

William S. Fletcher

Rolls-Royce North America, Indianapolis Indiana

e-mail: william.s.fletcher@rolls-royce.com

MIT 3rd STAMP/STPA Conference March 2014

Trusted to deliver excellence

Rolls-Royce

Rolls-Royce

Rolls-Royce

What do I do now that I have read the book?

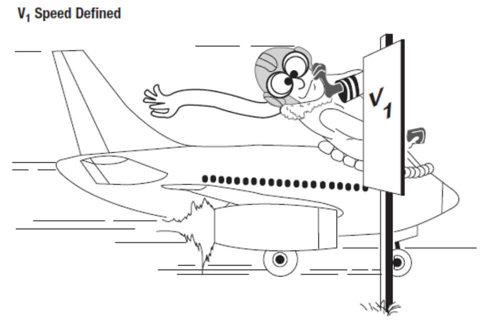
- Functions are being introduced to aircraft to ensure that the engine will respond to a reduction in throttle during a Rejected Takeoff (RTO)
- Review the historical context for protecting the aircraft under this condition and high level requirements for the protection system
- Flight test results drove retrospective analysis of the requirements using STPA
  - Found the issues that impacted flight testing plus others
  - The safety constrains and design considerations developed from the STPA analysis enable re-validation of the requirements
- Corrected software delivered to customers with delays between 3 and 12 months

While the material in this presentation is based on an actual system some details are changed to allow discussions with a wider audience. This may result in inconsistencies between slides.

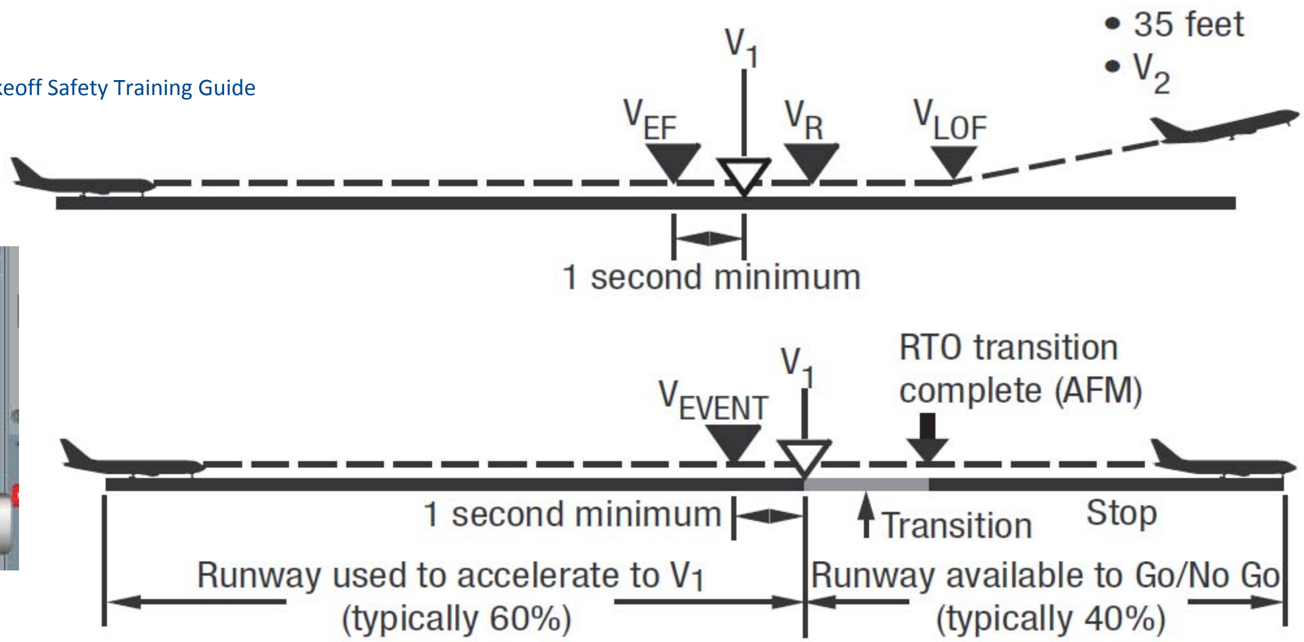
Rolls-Royce

Background – Rejected Takeoffs and V1 Decision speed

- Manufacturer's of passenger aircraft have to demonstrate minimum aircraft capabilities including
  - The ability to takeoff when one engine fails after V1
  - The ability to accelerate to V1 apply full brakes and come to a complete stop while remaining on the runway



FAA (1993) Takeoff Safety Training Guide



Air/Ground <air>

Air/Ground <ground>

Throttle

What happens during a rejected takeoff if one engine is stuck at high power and the others are at idle?

Rolls-Royce

Background - A Rejected Takeoff Accident

1997 Boeing B737 RTO at Najran

- During a normal takeoff, the flight-crew reject the takeoff at 120 knots
  - Thrust increase and over-temperature indication on right hand engine
- Flight-crew reduced power to Idle/Reverse on both engines
  - Right engine remained at takeoff thrust
  - Aircraft went off the end of the runway
- Aircraft suffered structural damage including collapse of main landing gear
  - Minor injuries occurred during the evacuation
  - Fuel leak lead to fire which destroyed the aircraft
- NTSB requests evaluation and corrective action, reference NTSB A-98-67 through -70

Najran, Saudi Arabia

Boston, MA

Rolls-Royce

Regulatory/Industry response to NTSB recommendations

(c) For each powerplant and auxiliary power unit installation, it must be established that <u>no single failure or malfunction or probable combination of failures will jeopardize the safe operation of the airplane</u> except that the failure of structural elements need not be considered if the probability of such failure is extremely remote.

- 14 CFR 25 Subpart E—Powerplant Sec. 25.901 Installation.

- Industry and regulatory committee evaluations
  - Single point mechanical failures within the engine fuel control and aircraft throttle system exist
  - For new engines practical designs exist to eliminate the failure mode
  - Existing engines with digital controls can be modified to detect the condition and shutdown the engine
  - Industry wide event rates all causes of ~3 events per 10 million flight hours (2001)
- For just the engine during takeoff, the hazard rate is on the order of 1 event per billion flight hours
- Regulatory view point – probability basis is not acceptable for new certification involving a single failure mode with catastrophic consequences
  - Design mitigation is required for new aircraft and existing aircraft when major changes are made
  - In 2010 implementation starts for TCM Protection on 2 small commercial engines

The result of these activities is a requirement for a new engine control function that we call Thrust Control Malfunction or TCM Protection

AIA/AECMA, 2002, Project Report on Strategies for Protection from Thrust Control System Malfunctions

Aircraft Hazard - Engine remains stuck at high thrust during a rejected takeoff, or landing rollout

TCM Protection- When the aircraft is on the ground during takeoff or landing, and fuel flow is stuck high, when the pilot moves Throttle (TLA) to the idle range, then automatically command an engine shutdown.

Engine requirements - When the aircraft is on the ground during takeoff or landing, and fuel flow is stuck high, when the pilot moves Throttle (TLA) to the idle range, then automatically command an engine shutdown.

System requirements

1. If a TCM event is detected disable engine starting
2. Prevent false TCM detection during normal transient operation throughout the flight envelope
3. Shutdown armed is true if air-ground switch is true and Throttle is at or below idle
4. If a TCM event is detected select alternate control law, if the TCM event persists and shutdown arm is true shutdown the engine

Software Requirements

Software Requirement

TCM Detection Algorithm

Software Requirement

Throttle (TLA) Signal Processing Algorithm

Software Requirement

Alternate Control Law Algorithm

Software Requirement

Air-ground signal Processing Algorithm

Software Requirement

Command engine shutdown

Requirements Hierarchy

Rolls-Royce

About two years later

“One test result is worth one-thousand expert opinions”
- Werner Von Braun

- Experimental flight test data shows TCM Protection detecting during flight above 20,000 feet
  - Not an unexpected result as engine response to throttle movement is slowed down above 20,000 feet
  - Air/ground switch protects engine from shutdown by TCM protection
- But what would happen if air/ground switch indicated ground when aircraft is in flight?
  - Engine control air/ground switch fault detection logic would not prevent shutdown for common mode failures under all conditions
- I read a book, I know what to do!
  - Retrospective review of the TCM function using STPA
  - The rest of this presentation discusses how the review was accomplished

STPA Step 1 - Define Accidents/Hazards

- Accidents use industry & regulatory definitions for loss
- Accident: During a rejected takeoff the aircraft departs runway due to high thrust caused by a thrust control malfunction
  - 1997 B737 Saudi Arabian Airlines RTO at Najran, one engine remained in full forward thrust one engine entered full reverse thrust NTSB A-98-67 through -70
- Hazard: Engine remains stuck at high thrust during a rejected takeoff

Rolls-Royce

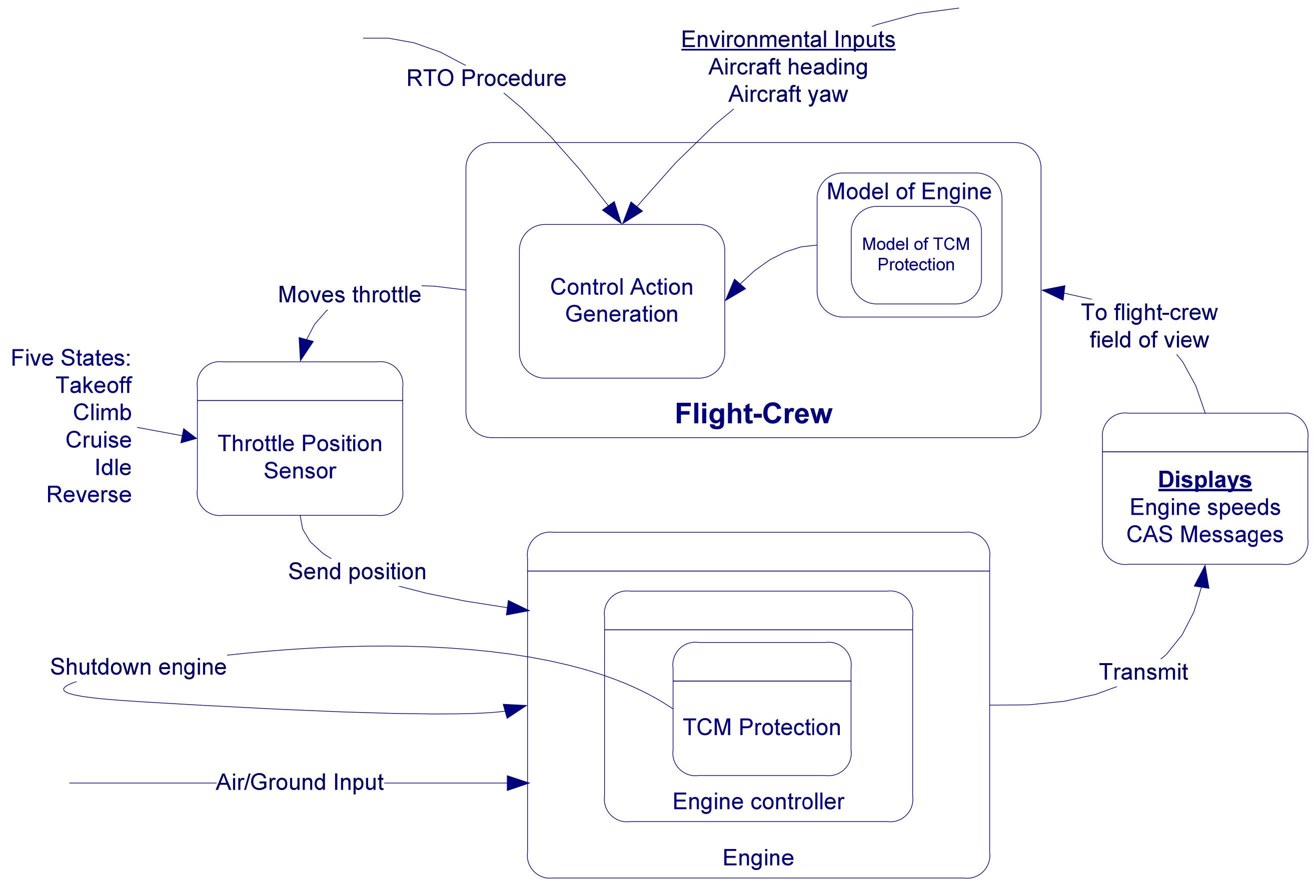
STPA Step 2A – Define unsafe control actions

Hazard: Engine remains stuck at high thrust during a rejected takeoff, or landing rollout					
Element	**Control Action**	**Providing causes hazard**	**Not providing causes hazard**	**Too early, too late, wrong order**	**Stopped too soon**
Aircraft	Provide forward thrust	During a rejected takeoff engine remains at high thrust (Runway departure)	If thrust is too low then the aircraft may fail to takeoff (Takeoff failure)		If the aircraft thrust is reduced by more than 1 engine (Takeoff failure)

Safety Constraint

When the aircraft is on the ground during takeoff or landing, and fuel flow is stuck high, when the pilot moves Throttle (TLA) to the idle, then automatically command an engine shutdown.

Safety Control Structure



Safety Constraint becomes the aircraft and engine requirements

When the aircraft is on the ground during takeoff or landing, and fuel flow is stuck high, when the pilot moves Throttle (TLA) to the idle, then automatically command an engine shutdown.

Rolls-Royce

Step 2A – Identify unsafe control actions

Hazard: Engine remains at high thrust during a rejected takeoff					
Element	**Control Action**	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, wrong order**	**Stopped too soon**
Flight-crew	RTO procedure reduce throttle (TLA) to idle	TCM Protection function not activated. Possible causes include TLA is reduced but not to idle, or wrong TLA is moved to idle (Runway departure)	---	Too late - Above V1 speed Wrong order – RTO above V_{Lof}, WOW is false then true (Runway departure)	TCM Protection function not activated. Possible causes include flight-crew moves TLA out of idle (TCM function may or may not activate depending on timing) (Runway departure)
TCM Protection (Process output)	Shutdown engine	During a rejected takeoff, engine remains at high power (Runway departure)	Aircraft in-flight, or Remote engine is shutdown (Inadvertent engine shutdown)	Too late - Aircraft is above V1	---

Rolls-Royce

System requirements for TCM Protection

System requirements

1. If a TCM event is detected disable engine starting
2. Prevent false TCM detection during normal transient operation throughout the flight envelope
3. Shutdown armed is true if air-ground switch is <ground> and throttle (TLA) is at or below idle
4. If a TCM event is detected select alternate control law, if the TCM event persists and shutdown arm is true shutdown the engine

- We sought to understand how the actions of the requirements for TCM Protection could lead to a hazardous control action
- Our approach was to take small portions (function groups) of the requirements (text or diagrams) and treat the internals of the implementation as a black box (i.e. how the specific behavior is implemented is not visible).
  - The purpose of the functional group becomes the control action
  - The concepts of provided not provided are extended to include: Output is wrong, or missing

Rolls-Royce

Unsafe control actions – System requirements (partial list)

Hazard: TCM Protection activates causing inadvertent engine shutdown

Requirement	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, wrong order	Stopped too soon
1. Starting	Inhibit	If fuel is stuck high during start: no start risk, or high temperature start, engine damage risk, or loud bang risk	Failure to start if aircraft is in-flight	---	---
3A. Read air-ground switch Position	Set *<ground>* (True) when on ground else set *<air>* (False)	Set *<air>* during rejected takeoff	Set <ground> when aircraft is in-flight	Late transition to *<air>* after takeoff or Late transition to *<ground>* after landing (prevents activation after landing)	---
3.B Throttle (TLA)	If TLA in *<Idle>* set True	If <Idle> is never true (signal faults, or TLA above idle)	If signal fault sets <Idle> (include thrust reverser interlock)	---	---
4.A Detect TCM Event	Set True if fuel flow is stuck high	During a rejected takeoff engine remains at high power (Runway departure)	TCM Event detected when aircraft is in-flight	Too late: if transition to alternate law is delayed, then engine shutdown is delayed	---
4.C Engine shutdown command	Shutdown engine	During a rejected takeoff engine remains at high power (Runway departure)	If the aircraft is in-flight or other engine is shutdown	Too late - If engine shutdown command is too late, aircraft will not slow down sufficiently (Runway departure)	---

Zoom in view – System requirements

Hazard: TCM Protection activates causing inadvertent engine shutdown			
Requirement	**Control Action**	**Not providing causes hazard**	**Providing causes hazard**
1. Starting	Inhibit	If fuel is stuck high during start: no start risk, or high temperature start, engine damage risk, or loud bang risk	Failure to start if aircraft is in-flight

System requirements

1. If a TCM event is detected disable engine starting

Rolls-Royce

Zoom in view – System requirements

Hazard: TCM Protection activates causing inadvertent engine shutdown			
Requirement	**Control Action**	**Not providing causes hazard**	**Providing causes hazard**
3A. Read air-ground switch Position	Set *<ground>* (True) when on ground else set *<air>* (False)	Set *<air>* during rejected takeoff	Set <ground> when aircraft is in-flight

System requirements

3. Shutdown armed is true if air-ground switch is <ground> and throttle (TLA) is at or below idle

Zoom in view – System requirements

Hazard: TCM Protection activates causing inadvertent engine shutdown

Requirement	Control Action	Not providing causes hazard	Providing causes hazard
4.A Detect TCM Event	Set True if fuel flow is stuck high	During a rejected takeoff engine remains at high power (Runway departure)	TCM Event detected when aircraft is in-flight

System requirements

4. If a TCM event is detected select alternate control law, if the TCM event persists and shutdown arm is true shutdown the engine

Rolls-Royce

Zoom in view – System requirements

Hazard: TCM Protection activates causing inadvertent engine shutdown			
Requirement	**Control Action**	**Providing causes hazard**	**Too early, too late, wrong order**
4.C Engine shutdown command	Shutdown engine	If the aircraft is in-flight or other engine is shutdown	Too late - If engine shutdown command is too late, aircraft will not slow down sufficiently (Runway departure)

System requirements

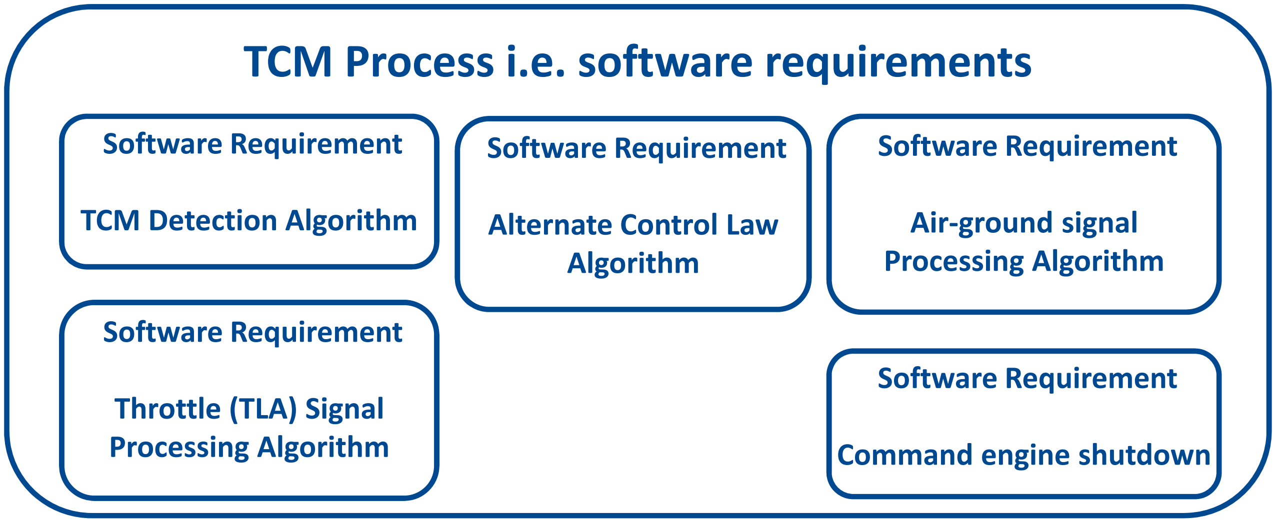
4. If a TCM event is detected select alternate control law, if the TCM event persists and shutdown arm is true shutdown the engine

Rolls-Royce

Analysis of software requirements – Unsafe control actions

> **"I have yet to see a problem, however complicated, which, when looked at in the right way, did not become still more complicated"**
> – Poul Anderson 1969

- Since we had detailed software requirements we also wanted to understand their potential for creating a hazardous control action
- We performed the unsafe control action analysis using the inputs, outputs, and functional action for each grouping
  - Place the input and output variables into the hazard table, along with a short action description
  - When doing unsafe control action and causal analysis on "black box" behavior assume that a design error exists and check the sufficiency of upstream requirements to prevent propagation of the error
  - Consider what would happen under each key word if the variables have the wrong state



Rolls-Royce

Software Requirements - Control Actions within the TCM Process

Hazard: TCM Protection activates causing inadvertent engine shutdown

Element ID	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, wrong order	Stopped too soon
Process Air/Ground signal	Set <*ground*> on ground else set <*air*>	Set <*air*> during rejected takeoff	Set <ground> when aircraft is in-flight	Late transition to <*air*> after takeoff or Late transition to <*ground*> after landing	---
TCM Dectection	Set True during TCM event	If the algorithm does not detect a TCM condition	If the algorithm detects another condition as a TCM condition	Too late: if transition to alternate law is delayed, then engine shutdown is delayed	---
Command engine shutdown	Shutdown engine	During a rejected takeoff engine remains at high power (Runway departure)	If the aircraft is in-flight or other engine is shutdown	Too late - If engine shutdown command is too late, aircraft will not slow down sufficiently (Runway departure)	---
Process Throttle (TLA) signal	If TLA in <Idle> set True	If <Idle> is never true (signal faults, or TLA above idle)	If signal fault sets <Idle> (include thrust reverser interlock)	---	---

Zoom in view – Software requirements

Hazard: TCM Protection activates causing inadvertent engine shutdown			
Requirement	**Control Action**	**Providing causes hazard**	**Too early, too late, wrong order**
TCM Dectection	Set True during TCM event	If the algorithm detects another condition as a TCM condition	Too late: if transition to alternate law is delayed, then engine shutdown is delayed

Software Requirement

TCM Detection Algorithm

Rolls-Royce

Zoom in view - Software requirements

Hazard: TCM Protection activates causing inadvertent engine shutdown			
Requirement	**Control Action**	**Not Providing causes hazard**	**Providing causes hazard**
Process Throttle (TLA) signal	If TLA in <Idle> set True	If <Idle> is never true (signal faults, or TLA above idle)	If signal fault sets <Idle> (include thrust reverser interlock)

Software Requirement

Throttle (TLA) Signal Processing Algorithm

Rolls-Royce

…but Step 2B causal analysis is still needed

- The approach above facilitated reuse of the existing software requirements
- Causal analysis is still needed to ensure completeness
  - Captures other information about the algorithm such as alternate control laws, fault detection and accommodation, timing, etc.
- Other requirement areas not related to a command action show up during casual analysis
  - Control Process: changes over time, engine response time changes with altitude and control modes
  - Component failures: The 3rd failure state for throttle sets position to idle, an action which enables TCM protection shutdown
  - Sensor: engine air/ground switch can be incorrect
  - Conflicting control actions: control is in alternate mode

Rolls-Royce

Air-ground switch – Inadequate operation

Process	Description	Description of Inadequate Operation	References
Aircraft Air-Ground switch	Set TRUE if aircraft is on ground, else set FALSE. Optional, set FAIL if system is known to be inoperative	**Incorrect False** - False during flight due to malfunction or maintenance error	Test equipment alters system behavior
		Incorrect True - True during flight due to malfunction or maintenance error	Test equipment alters system behavior Mars polar lander Maintenance set switch to on-ground, Gulfstream V, West Palm Beach, FL., Feb 14, 2002
		Wrong order - Bounces True-False-True - input changes state several times before settling in final state	Bounce landing with thrust reverser lockout, NTSB Report AAR1201
		Feedback Delay Late transition to false during initial phase of climb, or late transition to true during landing rollout	Failure accommodation for the aircraft WOW system can be based on a secondary sensor system, e.g. airspeed

Rolls-Royce

Fix inadequate operation of air-ground switch

Use additional inputs to determine if the 'environment' matches the anticipated process model for TCM Protection

Original Air-Ground Switch

	T
Air-ground switch – left	X
Air-ground switch – right	X

Safety Constraint - When the aircraft is on the ground during takeoff or landing, and fuel flow is stuck high, when the pilot moves Throttle (TLA) to the idle, then automatically command an engine shutdown

New On Ground Indication

	T
Air-ground switch – left	X
Air-ground switch – right	X
Landing gear down and locked – left	X
Landing gear down and locked – right	X
Altitude less than 15,000 ft. – left	X
Altitude less than 15,000 ft. – right	X
Airspeed less than Vr – left	X
Airspeed less than Vr – right	X

- These systems are separated at the aircraft level in left side and right side systems
- New indications uses 8 inputs with at least 2 pairs having no common mode faults

Rolls-Royce

Increase protection against process output contributes to hazard

Use additional inputs that prevent process output from contributing to a hazard

Original requirements

	T
Air-ground switch left	X
Air-ground switch right	X
Throttle (TLA) Channel A <= Idle	X
Throttle (TLA) Channel B <= Idle	X
TCM Event Detected Channel A	X
TCM Event Detected Channel B	X

Safety Constraint - When the aircraft is on the ground during takeoff or landing, and fuel flow is stuck high, when the pilot moves Throttle (TLA) to the idle, then automatically command an engine shutdown

Modified requirements

	T
On-ground indication Channel A	X
On-ground indication Channel B	X
Remote engine status Channel A running	X
Remote engine status Channel B running	X
Throttle (TLA) Channel A is at Idle	X
Throttle (TLA) Channel B is at Idle	X
Throttle (TLA) Channel A has no faults	X
Throttle (TLA) Channel B has no faults	X
TCM Event Detected Channel A	X
TCM Event Detected Channel B	X

The new requirements only allow one engine to automatically shutdown for a TCM event

Rolls-Royce

Summary

- Role of air/ground switch failure states was not fully recognized during the original design process
  - Inputs protecting against inadvertent activation had a common mode failure case
- Changed environment during flight at altitude allows Thrust Control Malfunction (TCM) detection
- STPA analysis identified
  - The inadequate operation of the air-ground switch
  - The TCM protection process output contributing the unsafe control action of inadvertent engine shutdown
  - Relative to the original design work STPA identified approximately 30 additional items that required review including several design changes
- Although a "novel" approach (STPA) applied techniques slightly different from the examples, the ability to explain the approach and understand the results drove consensus for the solutions
- Improved software now in customer's flight tests with no TCM functional issues. Aircraft level approval for both engines in 2014.

Rolls-Royce