USE OF THE STPA TECHNIQUE IN THE REQUIREMENTS DEFINITION OF A DRONE POWER GENERATION SYSTEM

2022 MIT STAMP Workshop

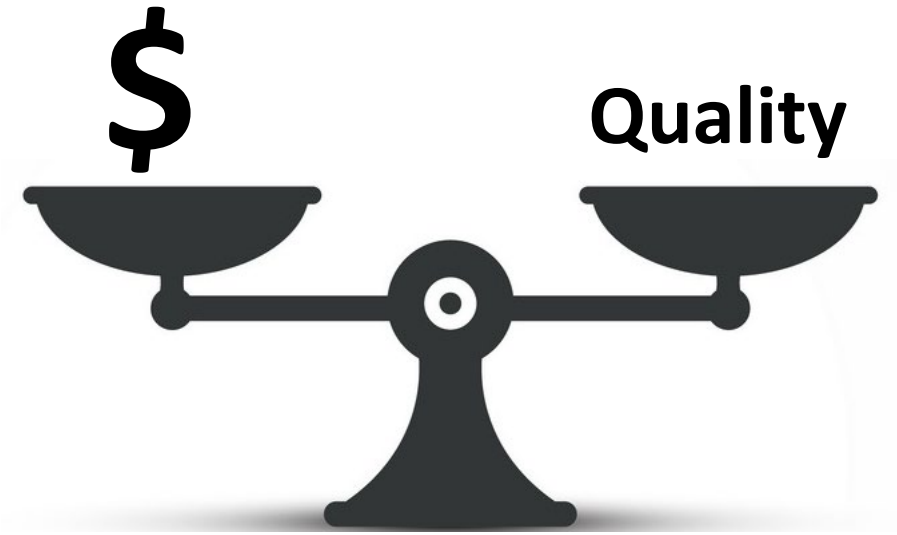
Presentation Topics

- Why STPA
- Case Study
  - Loss
  - Hazards
  - Control Diagram
  - Modes in States
  - Unsafe Control Action
  - Causal Scenarios
  - Requirements
- Real Results
- Maintenance Activity
- Next steps
- Contributions

Why STPA

Project Time ⇨ **Quality** ⇨ **Product Cost**

FTA
FEMEA
X
STPA



UNIFEI Universidade Federal de Itajubá xmobots® Massachusetts Institute of Technology

Case Study

Aircraft Level Losses

	Loss	Definition
A-1	Loss or significant damage to the aircraft	Loss of the entire aircraft or significant damage that does not allow maintenance in the field and by the operator himself
A-2	Significant damage to other people's property	Damage to third party equipment integrated into the aircraft and/or damage to third party property (fire) and property.
A-3	Fatalities or injury to persons	Causing death or significant damage to human lives.
A-4	Mission Non-Compliance	Complete non-fulfillment of the established mission, damaging the image of the product.

Case Study

Aircraft Level Losses

	Loss	Definition
A-4	**Mission Non-Compliance**	**Complete non-fulfillment of the established mission, damaging the image of the product.**

Case Study

Aircraft Level Hazards

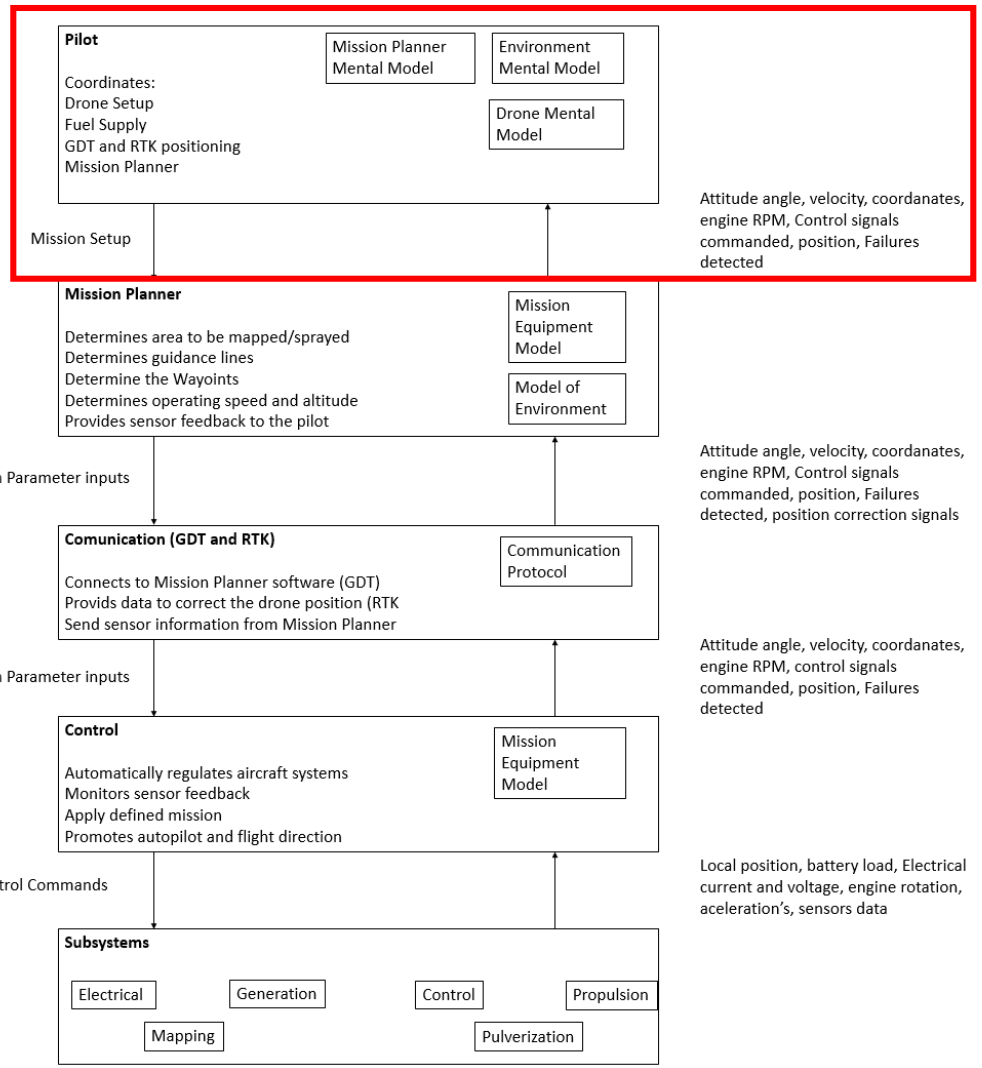
	Hazard	Definition	Safety Constraint	Loss
H1	The aircraft violates the minimum safety distance	Aircraft gets too close to obstacles during its mission (trees, terrain, building...).	Aircraft should maintain a safe distance from obstacles and notify the operator when reaching the minimum distance.	A-1; A-2; A-3; A-4
H2	The aircraft loss the communication with base	Aircraft cannot receive or/and send data to base.	The aircraft must maintain constant communication with the base throughout the operation.	A-1; A-2; A-3; A-4
H3	The aircraft have insufficient power available	Aircraft loses the ability to generate power enough to supply the aircraft needs, making the battery voltage to drop below the minimum required.	The aircraft must be able to generate enough power to keep the systems running properly.	A-4; A-1
H4	The aircraft loss the flight capability	Aircraft is not able to maintain flight, or perform controlled takeoff and landing, during operation.	Aircraft shall be capable of remaining airborn in a controlled manner throughout the operation.	A-1; A-2; A-3; A-4

Case Study

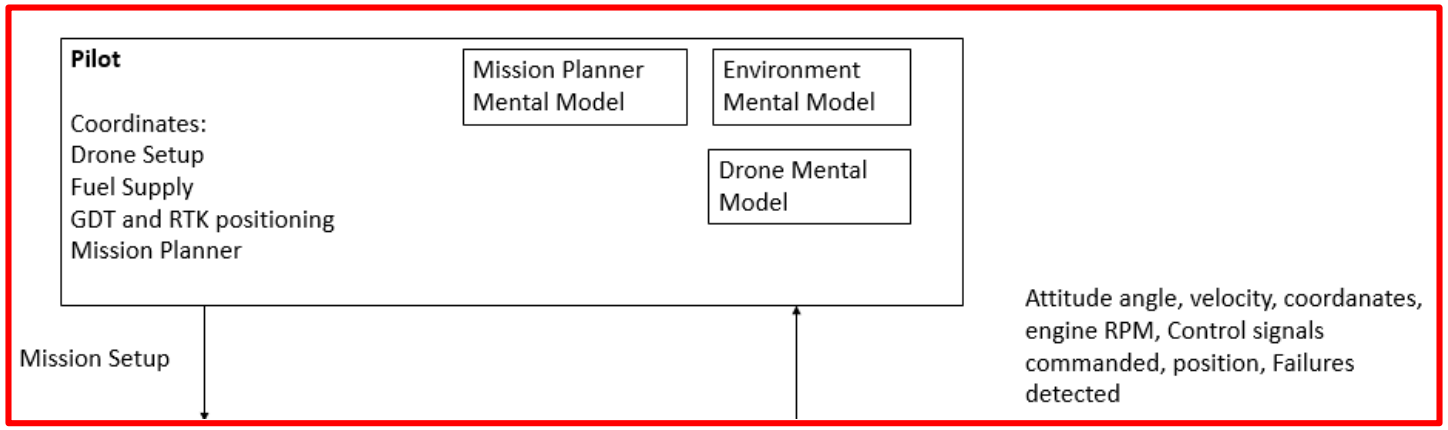
Aircraft Level Hazards

	Hazard	Definition	Safety Constraint	Loss
H3	The aircraft have insufficient power available	Aircraft loses the ability to generate power enough to supply the aircraft needs, making the battery voltage to drop below the minimum required.	The aircraft must be able to generate enough power to keep the systems running properly.	A-4; A-1

Case Study



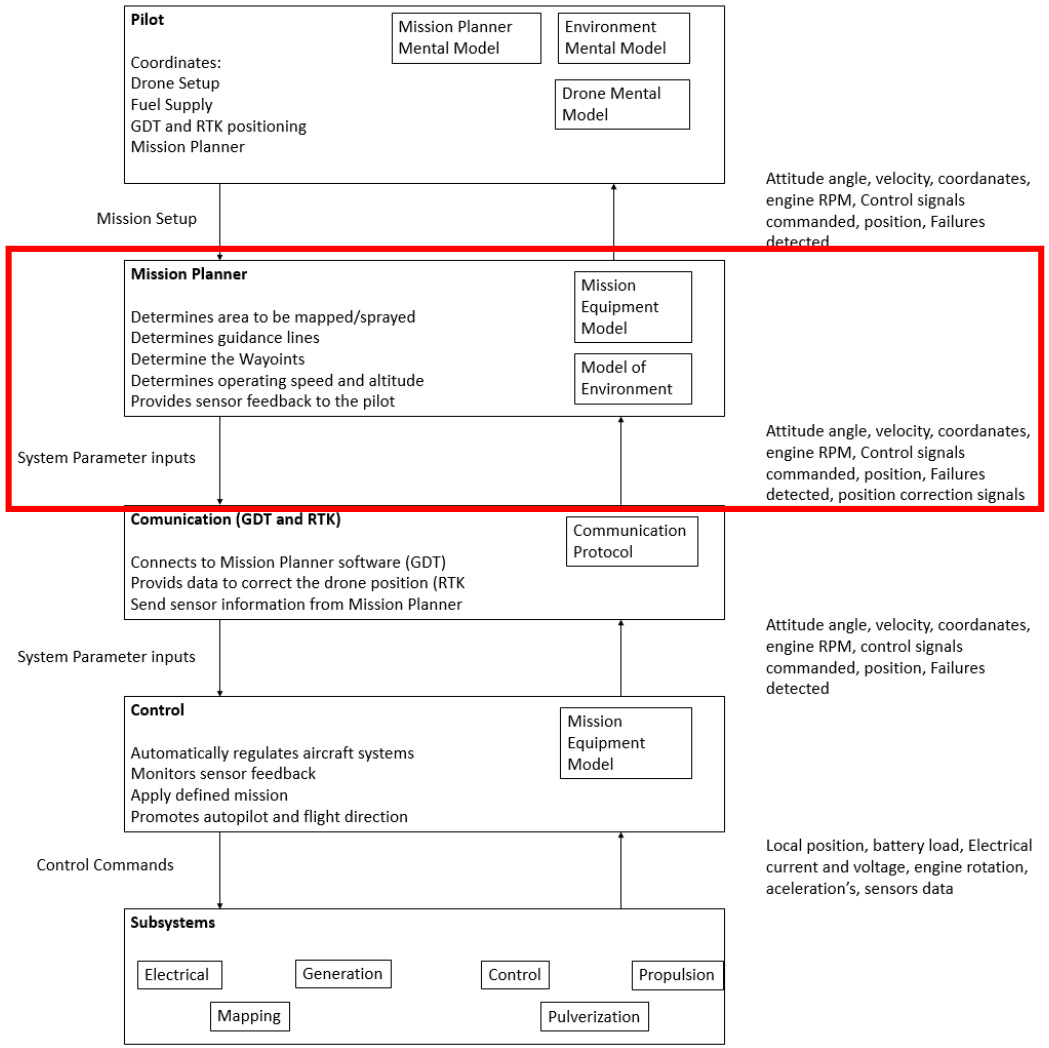
Aircraft Level Control Diagram

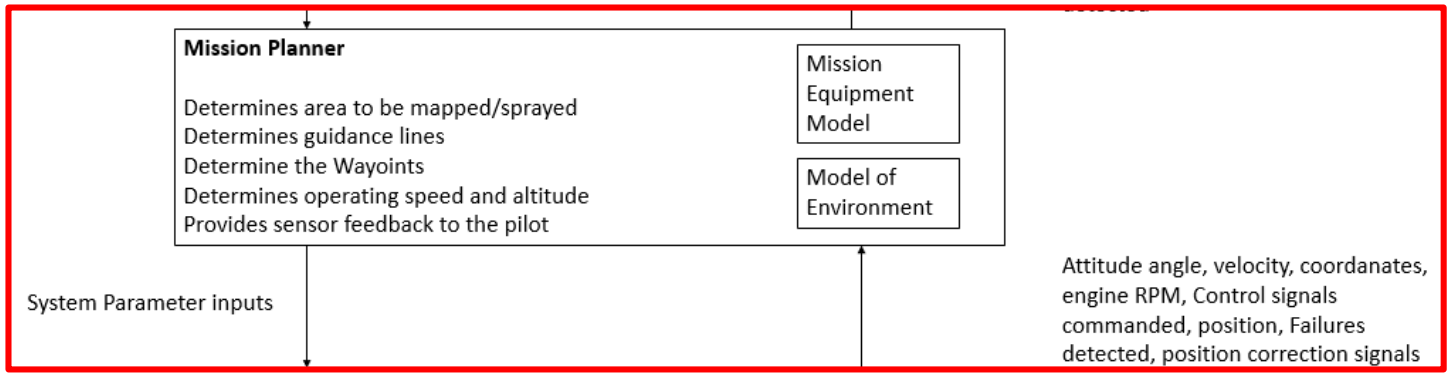


UNIFEI Universidade Federal de Itajubá xmobots® Massachusetts Institute of Technology

Case Study

Aircraft Level Control Diagram

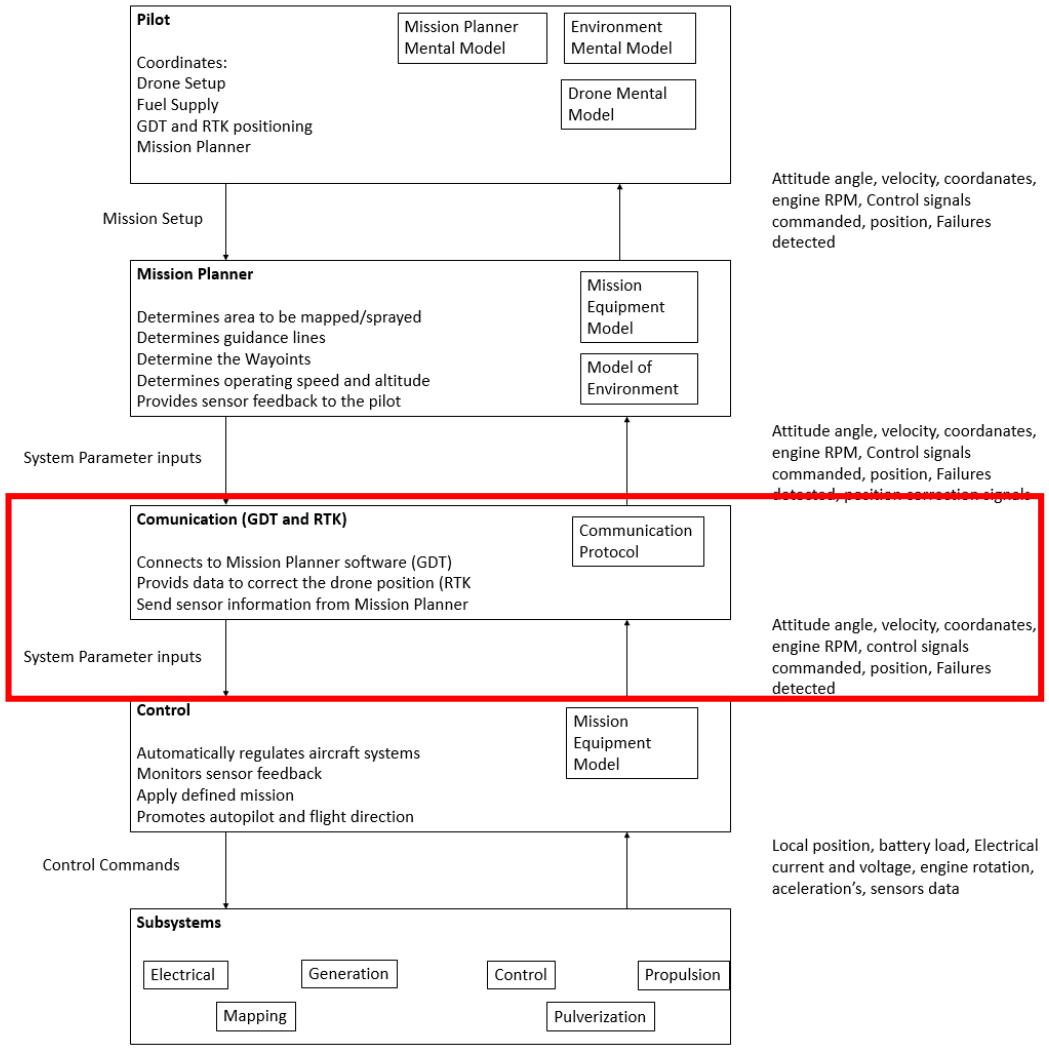


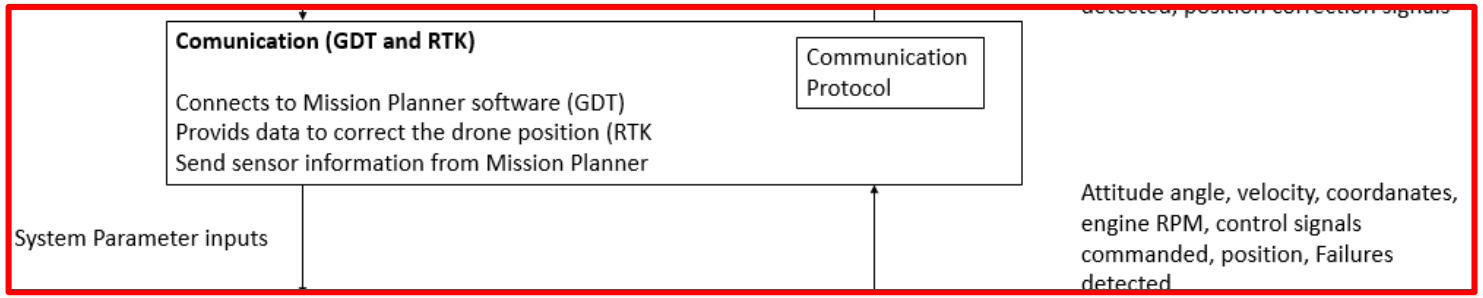


UNIFEI Universidade Federal de Itajubá xmobots® Massachusetts Institute of Technology

Case Study

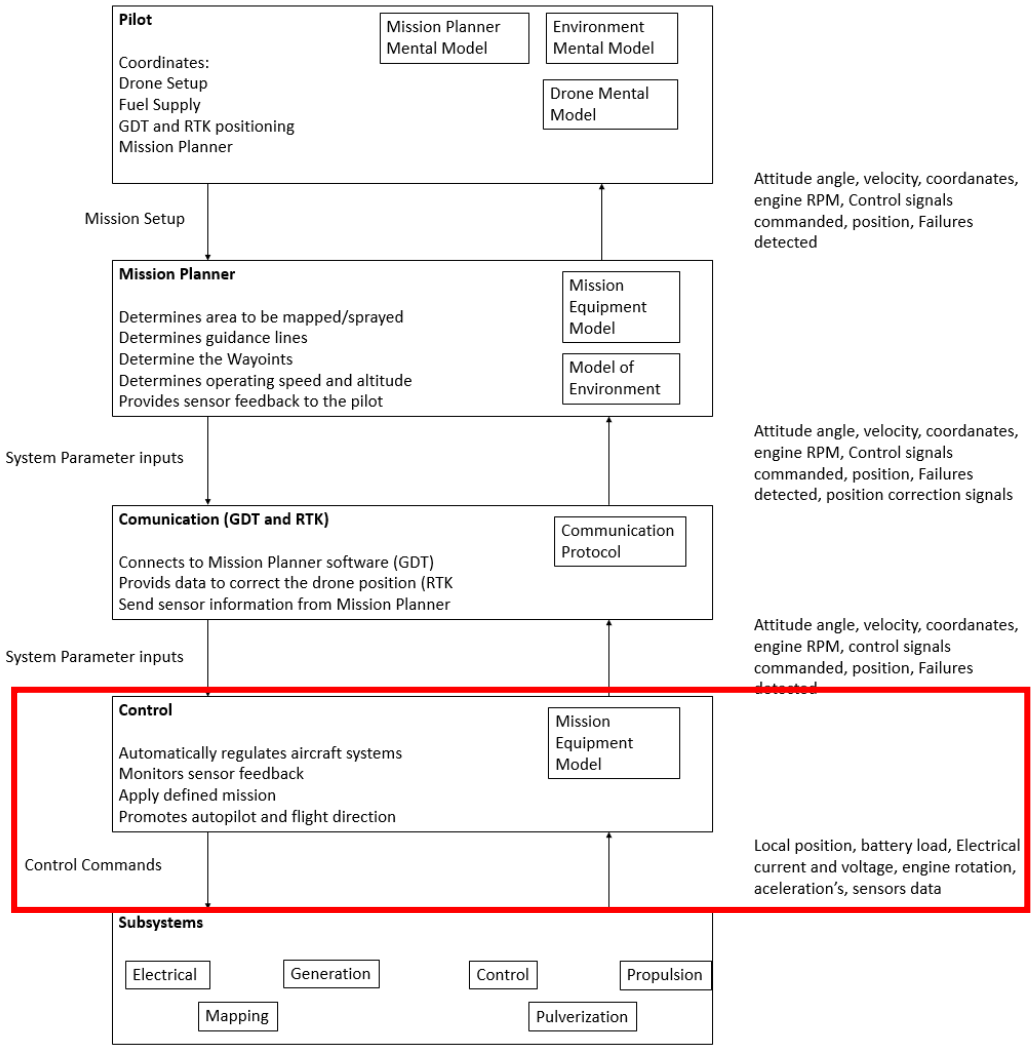
Aircraft Level Control Diagram

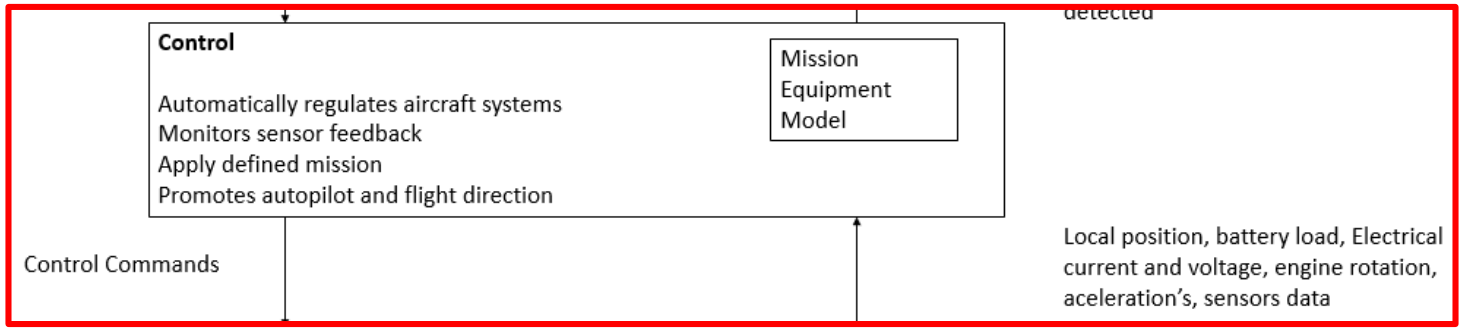




Case Study

Aircraft Level Control Diagram

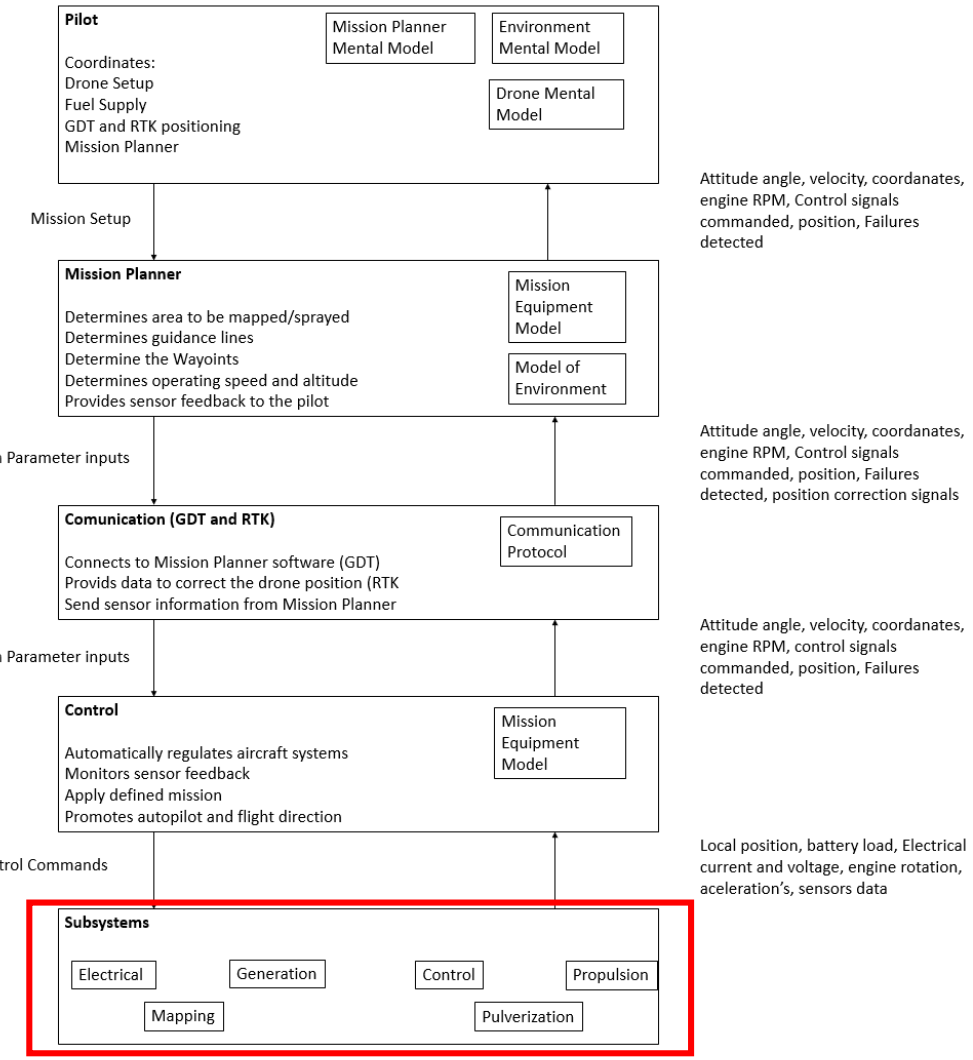




UNIFEI Universidade Federal de Itajubá xmobots® Massachusetts Institute of Technology

Case Study

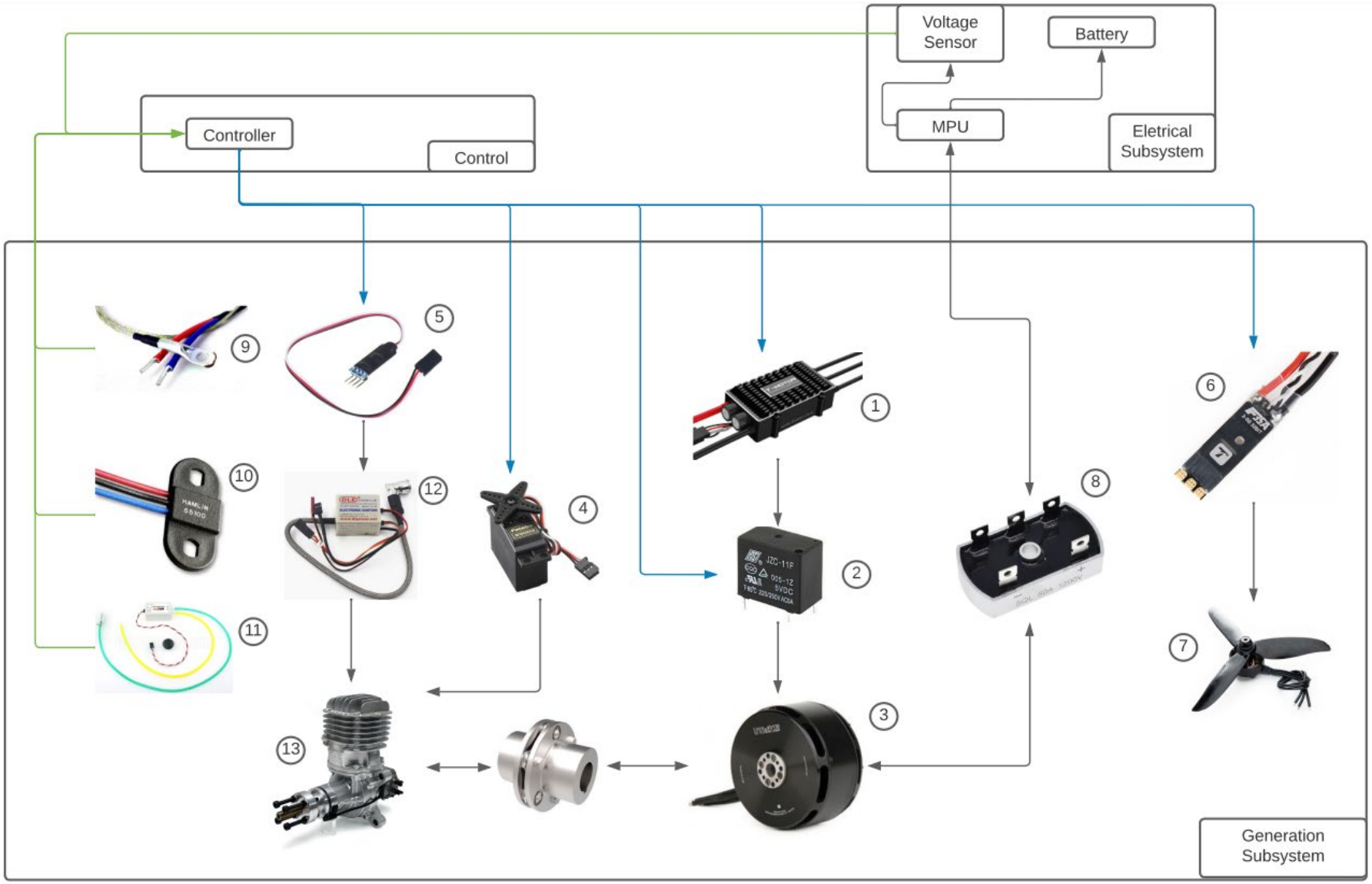
Aircraft Level Control Diagram



UNIFEI Universidade Federal de Itajubá xmobots® Massachusetts Institute of Technology

Case Study

Generation System Control Diagram

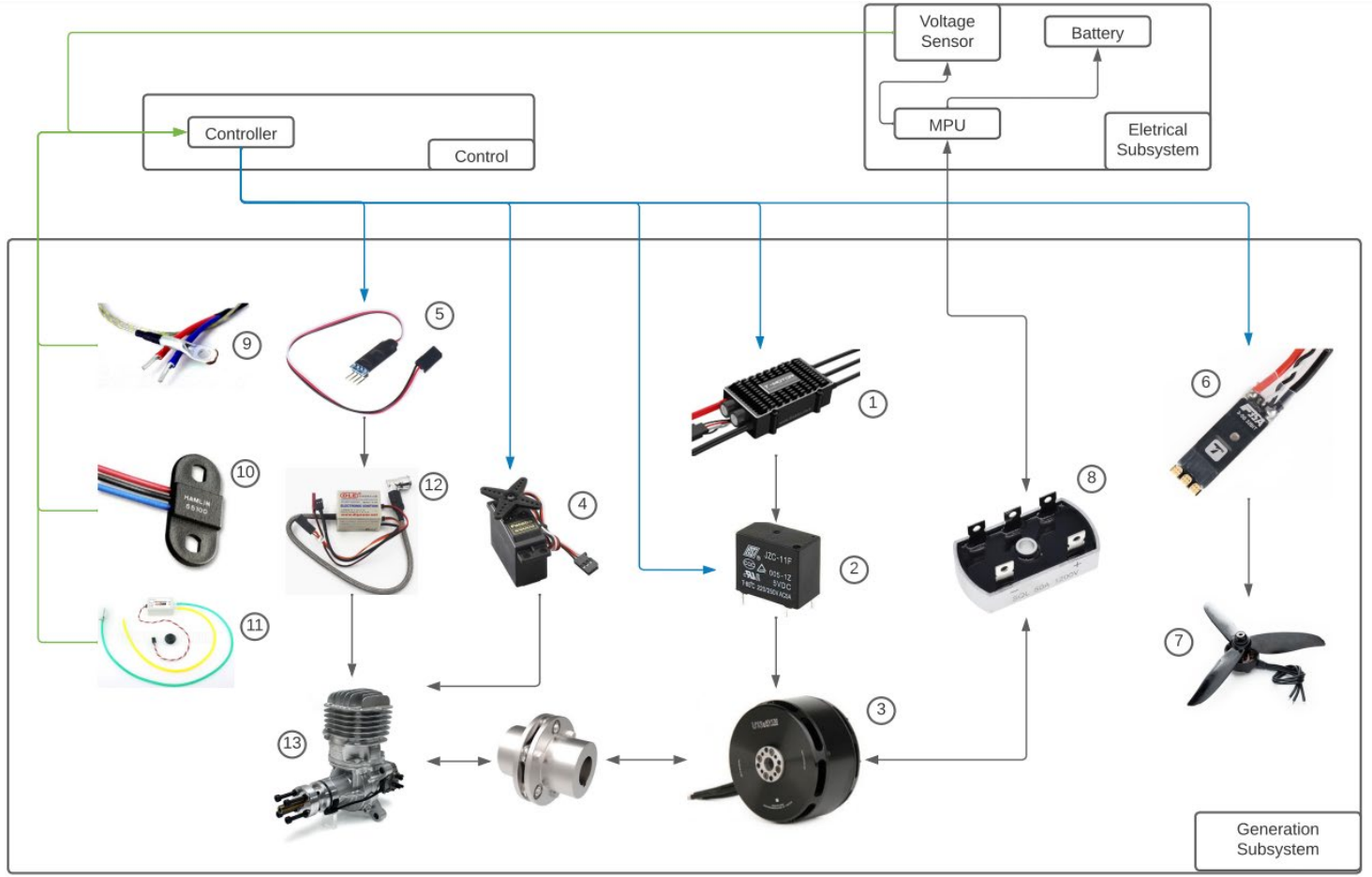


UNIFEI Universidade Federal de Itajubá xmobots® Massachusetts Institute of Technology

Case Study

Generation System Control Diagram

- The electric motor (3) at first is used to start the combustion engine (13)
- The relay (2) closes the contact and allows the connection between the ESC (1) and electric motor
- The actuator (4) is in the idle position and the kill-switch (5) is off.
- The controller send the PWM signal to the ESC of the fan (6), turn-on the fan (7).

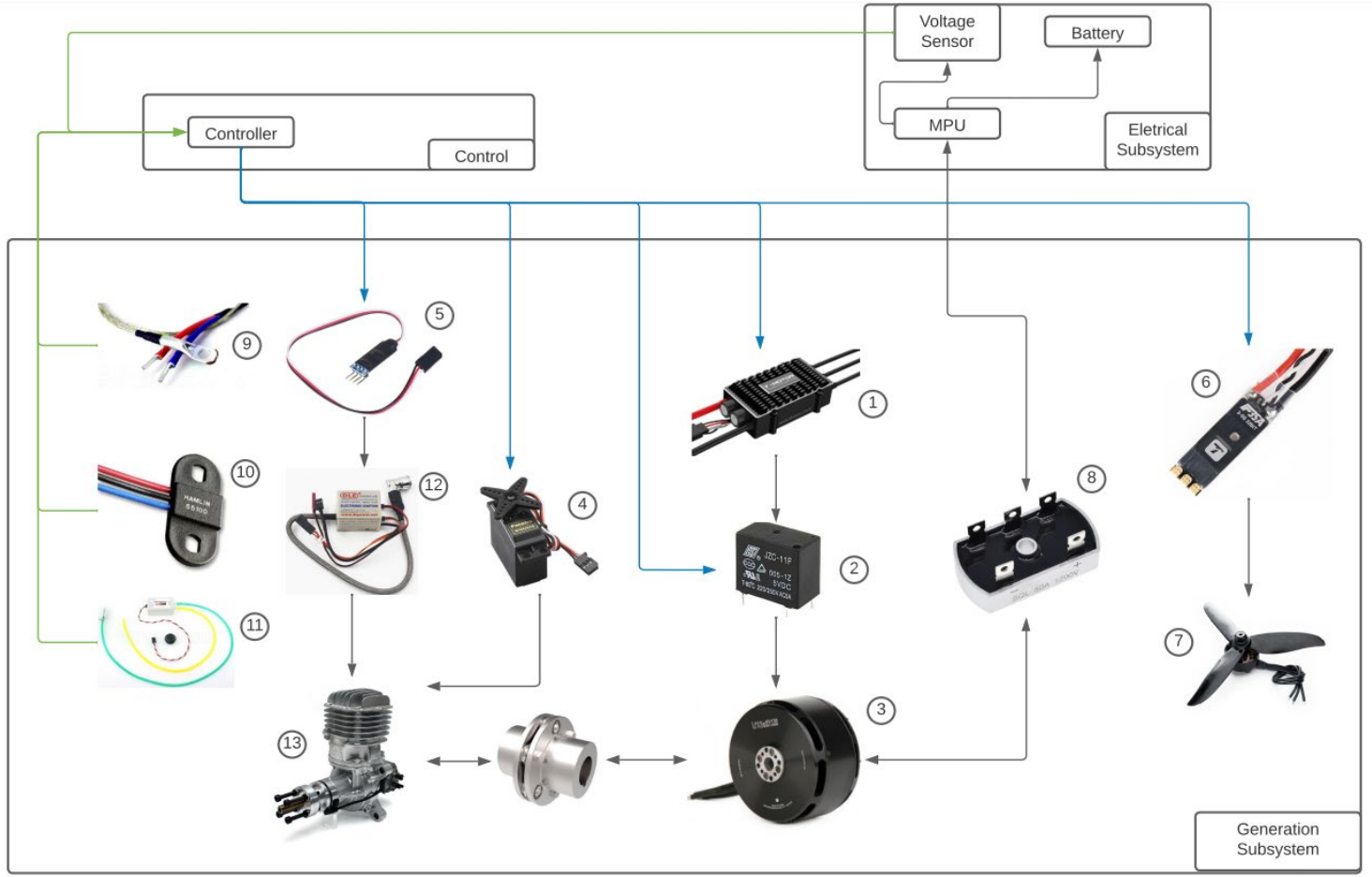


UNIFEI Universidade Federal de Itajubá xmobots® Massachusetts Institute of Technology

Case Study

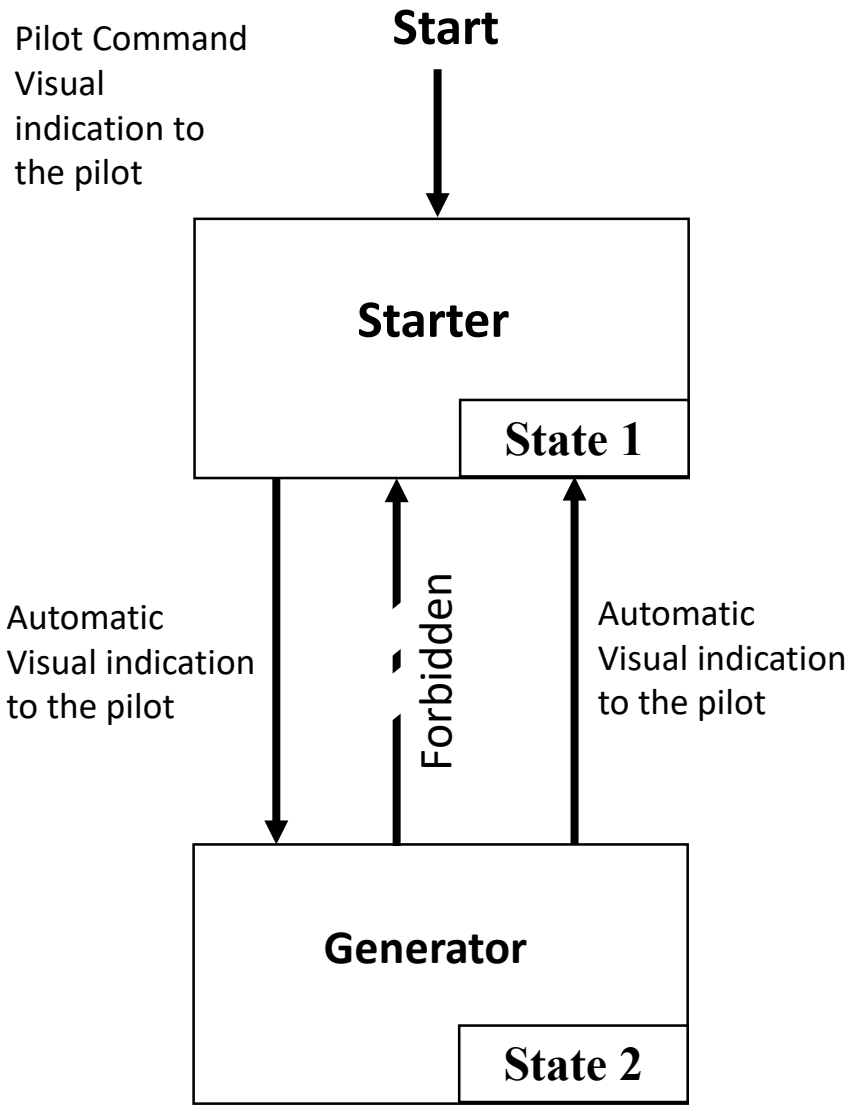
Generation System Control Diagram

- The rectifier (8) is responsible to convert the AC (alternate current) to DC (direct current)
- The feedback from the sensors (temperature (9); RPM (10); Fuel (11)) is presented continuously to the operator during the entire mission
- The controller commands to finish the mission, then a signal is sent to cut the ignition power (12), activate the Kill-Switch, turning off the combustion engine
- Identified that the engine is off, the controller turn-off the fan.



UNIFEI Universidade Federal de Itajubá xmobots® Massachusetts Institute of Technology

Case Study



Modes in States

Control Action	Not providing a control action leads to a hazard	Providing a control action leads to the hazard	A control action provided with incorrect timing or in the wrong order creates the hazard	A control action stopped too soon or applied for too long
Transition Mode 1 to Mode 2	**UCA A01** The controller does not command the transition from mode 1 to mode 2		**UCA A02** The controller commands to change from mode 1 to mode 2 after the drone takeoff	
Transition State 2 to State 1	**UCA A03** After the mission is completed, the controller does not change the state 2 to state 1	**UCA A04** The controller commands the transition from state 2 to state 1 during the mission		
Transition Mode 2 to Mode 1		**UCA A05** The controller commands the transition from mode 2 to mode 1 in flight		

Case Study

Control Actions

Starter

Generator

Control Action	Not providing a control action leads to a hazard	Providing a control action leads to the hazard	A control action provided with incorrect timing or in the wrong order creates the hazard	A control action stopped too soon or applied for too long
Switch "on" the fan		UCA 01 Controller runs the fan while the combustion motor is off		
Driving the Electric motor	UCA 02 The controller does not drive the electric motor as a starter function for the combustion engine, when command by the pilot	UCA 03 The controller drives the electric motor below the rotation required to start the combustion engine, when command by the pilot		UCA 04 Driving the electric motor as a starter for a long time, even after the combustion engine has started UCA 05 Driving the electric motor for a short period, not starting the combustion engine
Drive activate kill-switch		UCA 06 The controller actuates the kill-switch during starter		
Activate Relay	UCA 7 The controller does not actuate relay (closing the contact)			UCA 08 The controller keeps the relay closed for a short period
Command the servo	UCA 09 The controller does not actuate the throttle servo to idle/start position			
Start the Combustion Engine	UCA 10 Do not start Combustion Engine, when commanded by the pilot.			

Control Action	Not providing a control action leads to a hazard	Providing a control action leads to the hazard	A control action provided with incorrect timing or in the wrong order creates the hazard	A control action stopped too soon or applied for too long
Switch "on" the fan	UCA 11 The Controller does not start the fan after the combustion engine has started running	UCA 12 Controller runs the fan below the speed required to cool the engine		
Keeping the motor as generator (mode 2)		UCA 13 The controller drives the electric motor as starter (mode1)		
Drive Activate kill-switch	UCA 14 The controller does not actuate kill-switch after mission completion	UCA 15 The controller actuates the switch during aircraft mission accomplishment		UCA 16 The controller actuates the kill-switch for a short period, before the mission is completed
Activate Relay		UCA 17 The controller actuate relay during aircraft mission accomplishment		
Command the servo	UCA 18 The controller does not actuate the throttle servo as necessary to supply the power consumption during the mission		UCA 19 The controller operates the servo after the required/appropriate time required	UCA 20 Keep the servo feed after the end of the mission
Keep the engine running	UCA 21 The controller does not disactivate the combustion engine after the mission is finished	UCA 22 The controller disactivate the combustion engine during the mission		

UNIFEI Universidade Federal de Itajubá xmobots® Massachusetts Institute of Technology

Case Study

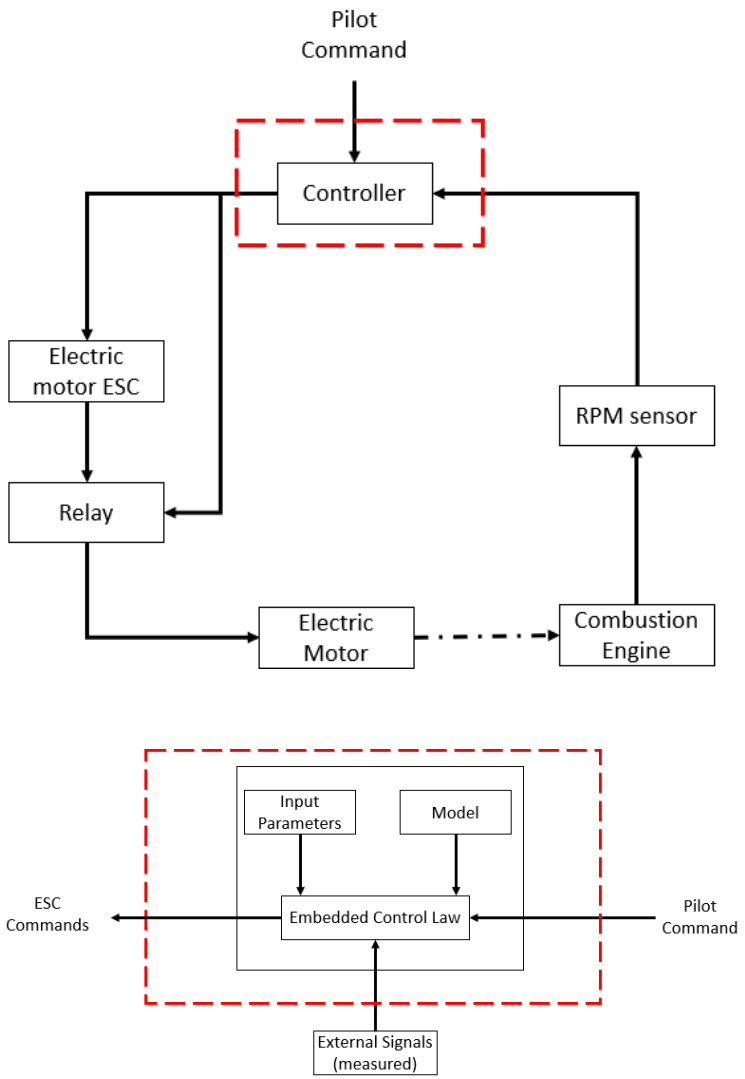
Starter

Control Action	Not providing a control action leads to a hazard	Providing a control action leads to the hazard	A control action provided with incorrect timing or in the wrong order creates the hazard	A control action stopped too soon or applied for too long
Driving the Electric motor	**UCA 02** The controller does not drive the electric motor as a starter function for the combustion engine, when command by the pilot	**UCA 03** The controller drives the electric motor below the rotation required to start the combustion engine, when command by the pilot		**UCA 04** Driving the electric motor as a starter for a long time, even after the combustion engine has started **UCA 05** Driving the electric motor for a short period, not starting the combustion engine

Generator

Control Action	Not providing a control action leads to a hazard	Providing a control action leads to the hazard	A control action provided with incorrect timing or in the wrong order creates the hazard	A control action stopped too soon or applied for too long
Keeping the motor as generator		UCA 13 The controller drives the electric motor as starter (mode1)		

Case Study



UCA03

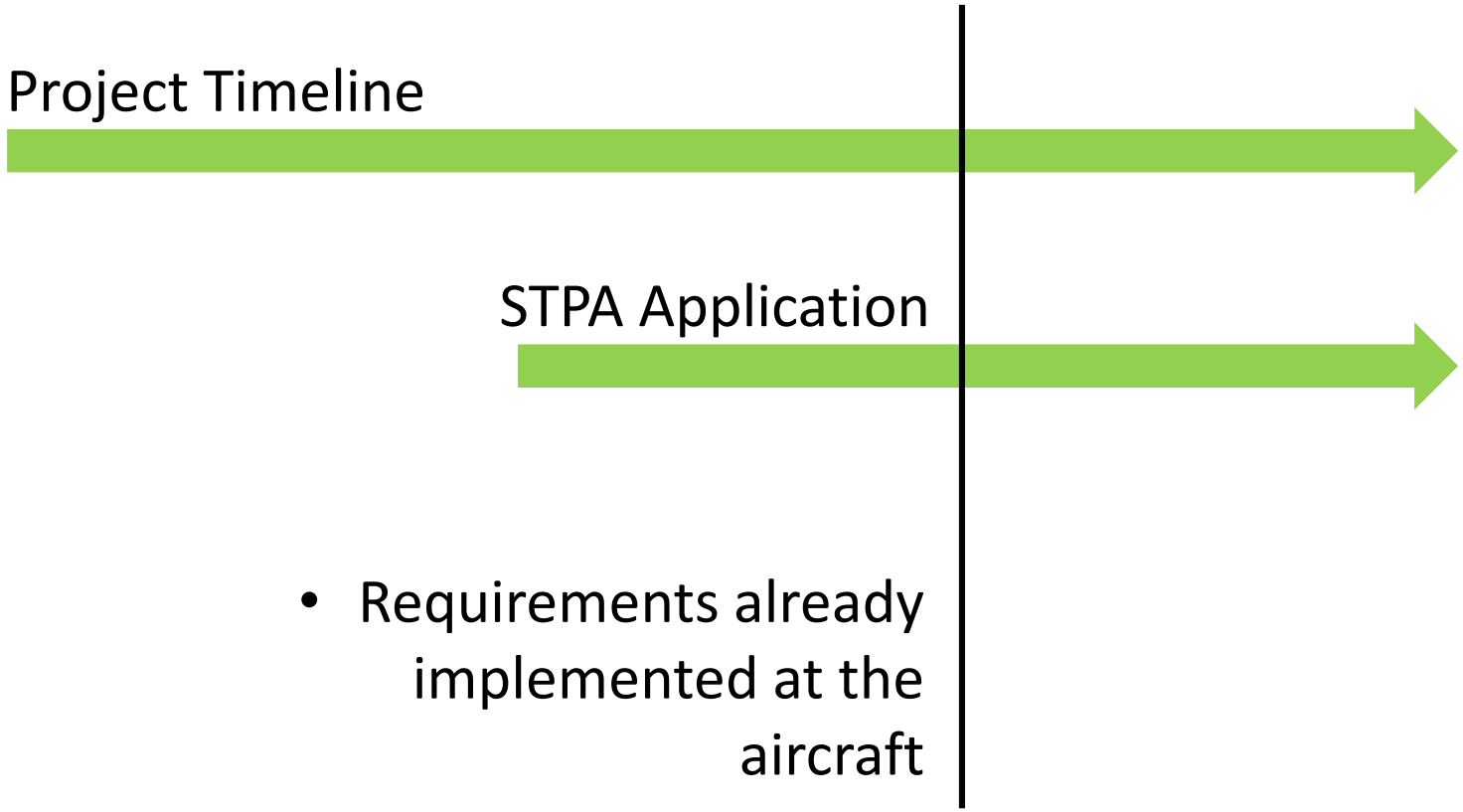
- The controller calculates correctly and sends the wrong PWM signal to the ESC, which in turn drives the low-speed electric motor.
- The inserted parameter at the controller is wrong, and, as consequence, the controller sends the wrong PWM signal.
- The controller sends the right PWM value, but the ESC receives the wrong value, as consequence of noise between both.
- The controller control law was correctly designed, but the embedded control law contains errors obtained during the compilation process.
- The electronic processor in which the controller law is embedded contain failures.

Case Study

Requirements

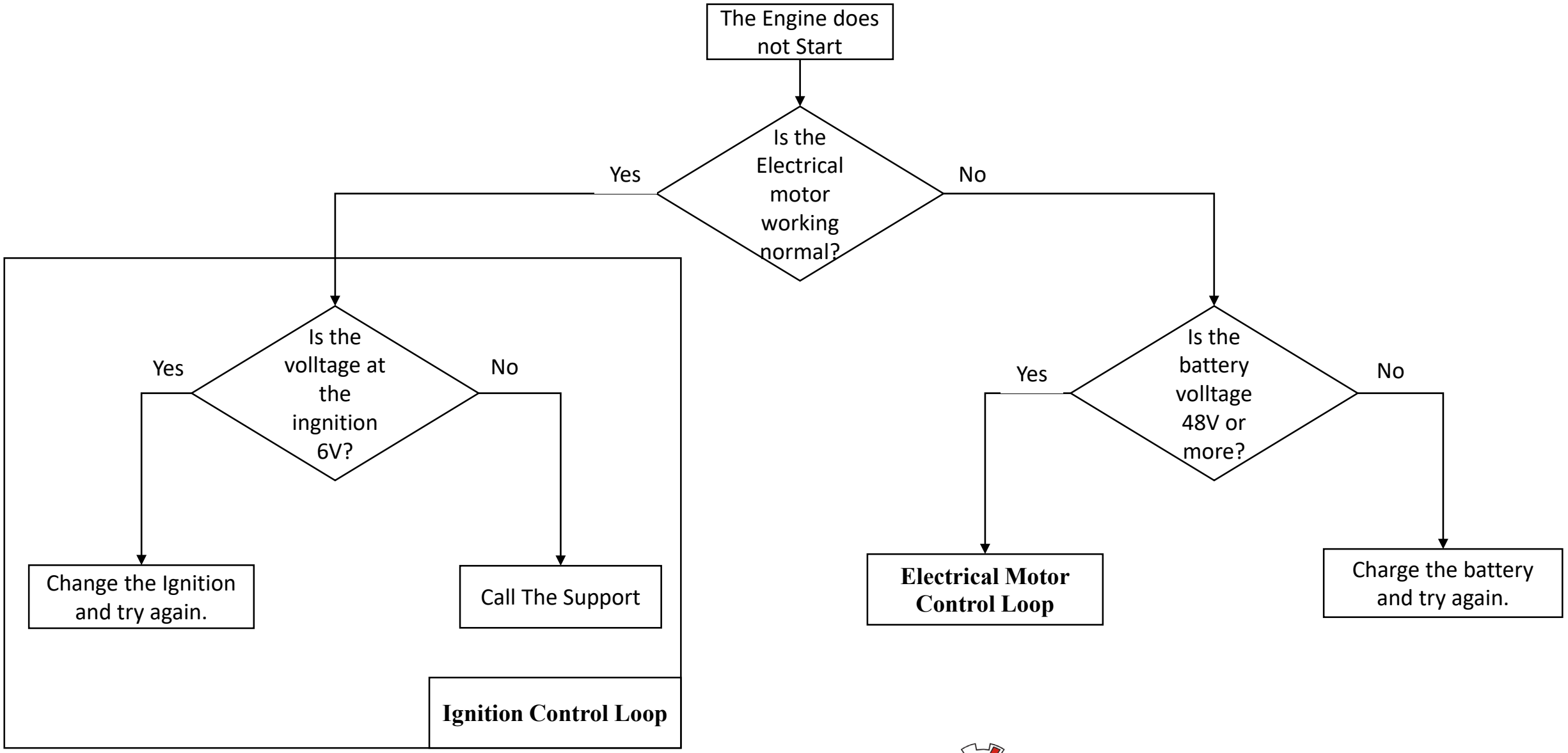
RF9	The controller must be able to start the electric motor, keeping it running for 5 seconds, when commanded to start by the operator.
RF10	After the 5 seconds the controller should be able to identify if the combustion engine is running. If not, 3 more attempts should be made.
RF11	The controller should be able to identify the engine start failure and send a signal to the flight planning software.
RF12	The PWM signal sent by the controller to the ESC of the electric motor must be sufficient to start the combustion engine.
RF13	The ESC+Electric motor assembly must be capable of operating at least 100 continuous hours without failure of any nature.
RF14	The signal to start the electric motor must be sent if, only if, the relay is open energized, contact closed.
RF15	Combustion engine failure should be indicated if the RPM sensor and the battery voltage sensor indicate it.
RF16	The mission should not be initiated until the engine start is confirmed.
RF17	Operational procedures are developed to certify that the input parameters defined by the pilot/ operators are correct.
RF18	The controller internal model must be validated before the controller design.
RF19	The controller requirements must be validated to attend the pilot, operator objectives.
RF20	Verification effort must be done to guarantee that the software architecture attends the software requirements.
RF21	Verification effort must be done to guarantee that the embedded software has the same behavior as the software designed.
RF22	There must be operational procedures to take note of any abnormal drone behavior and to communicate it to the drone manufacturing company.

Real Results



- New Requirements
- More Robust Product
- Development Cost Reduction

Maintenance Activity



Next Steps

- Buyout components
- Providers
- Software Code
- Assembly Process

Contributions

- Application of the STPA technique on the drone industry.

- The requirements obtained by applying the STPA allow to obtain a robust product at a low cost.

- The guidance promoted by the application of the STPA technique can assist in the aircraft maintainability.

- The STPA presents a very robust methodology, which covers much more than component failures, **addressing mainly failures between component interactions**. And by presenting an excellent guidance, it allows a fast and efficient analysis, reducing project costs.

Paulo Victor Meneguite Mendes

Xmobots - Brazil

paulo_meneguite@outlook.com

Marcelo Santiago de Souza

UNIFEI - Brazil

marcelo.santiago@unifei.edu.br

UNIFEI Universidade Federal de Itajubá xmobots® Massachusetts Institute of Technology

ITE MISSA EST

THANKS