

# MATLAB EXPO

 FRANCE

8 octobre 2024 | Paris

---

## Master Class : analyse précoce et continue de la sûreté de fonctionnement

*Magnus Nord, MathWorks*



Application Engineer

*Daniel Martins, MathWorks*



Application Engineer



# Agenda

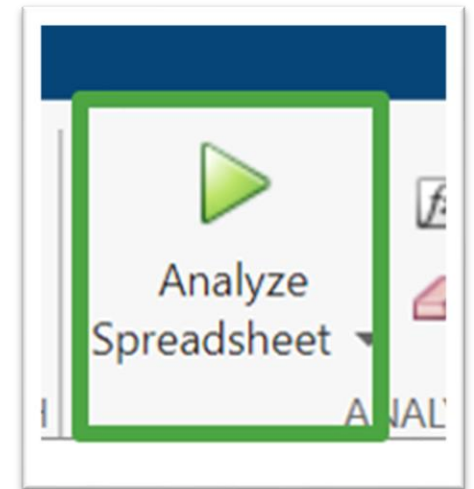


Background

or Extended X

	Failure	Local Effect	System Effect	S	Po
Pressure	Incorrect value	Incorrect pressure control.	Possible barotrauma.	8	8
		Higher than control pressure if control pressure is falsely lower.			

Problem Definition



Solution

GETINGE 



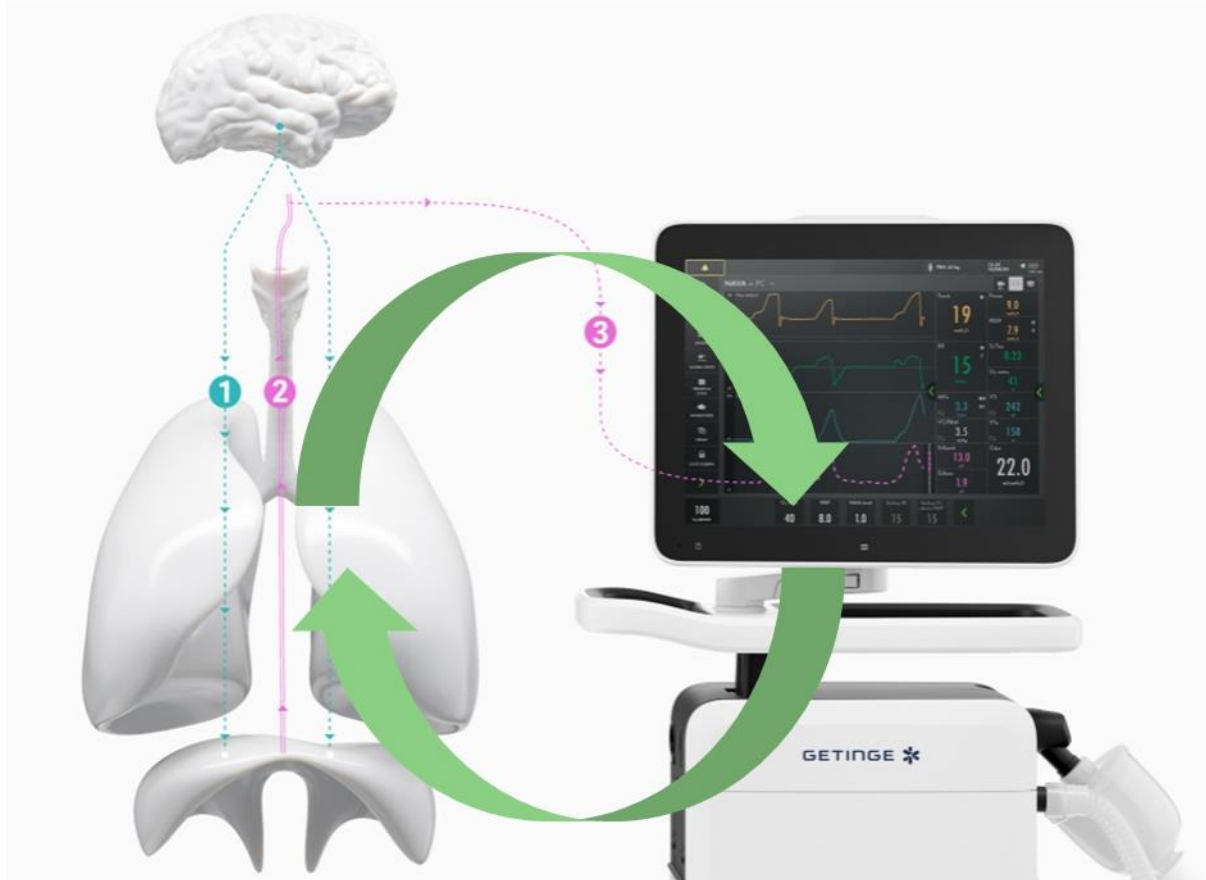
Anesthesia Machine

- Founded in 1904
- 12000 employees
- 40 countries
- First ventilator with valves and control loops.
- The world's first Implantable Pacemaker

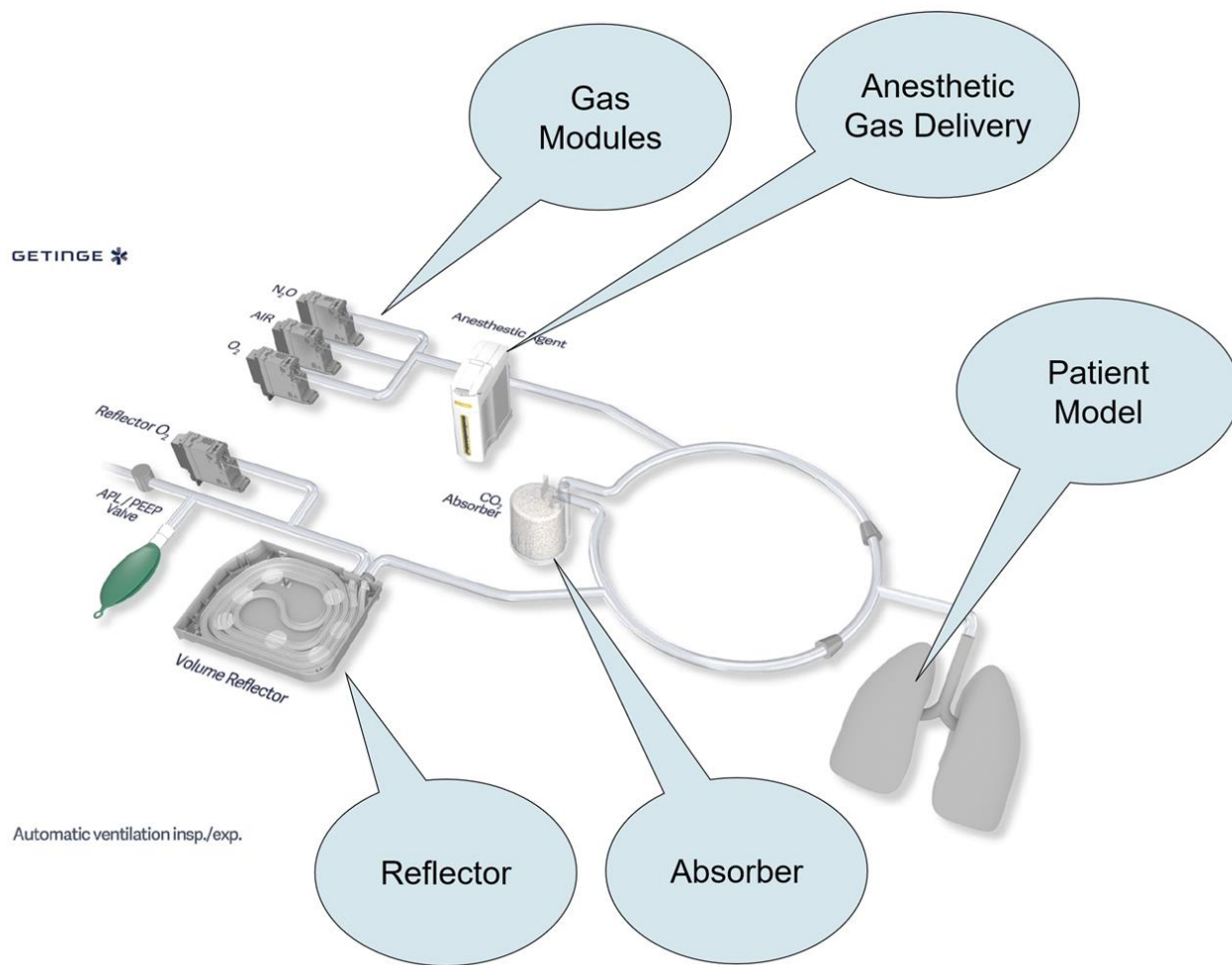


Mechanical Ventilator

# Getinge

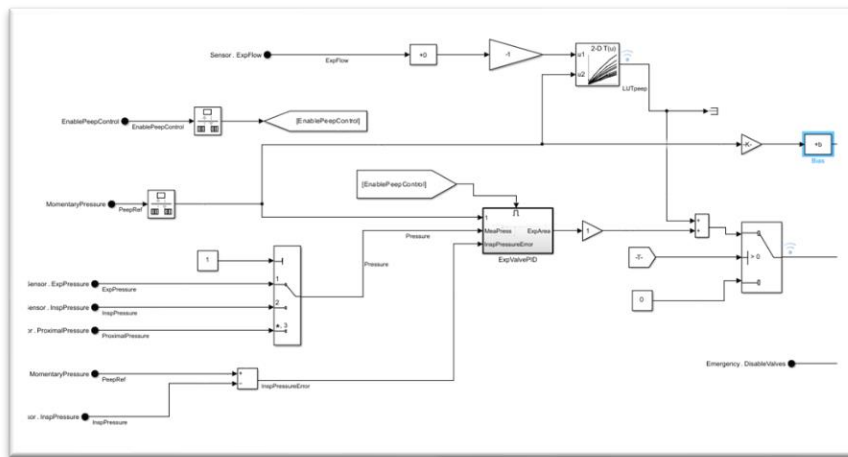
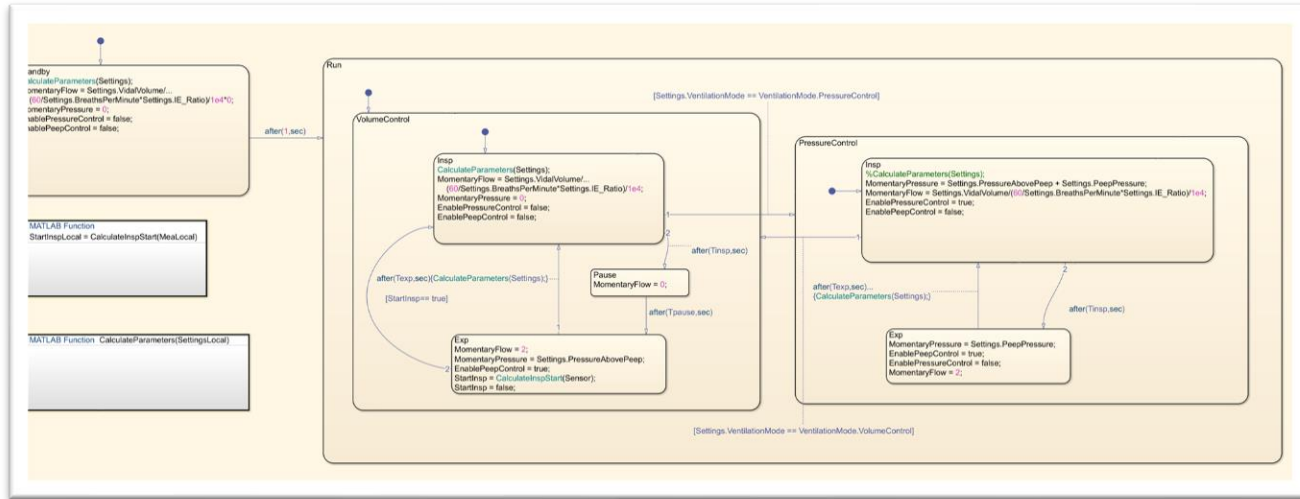


# Getinge

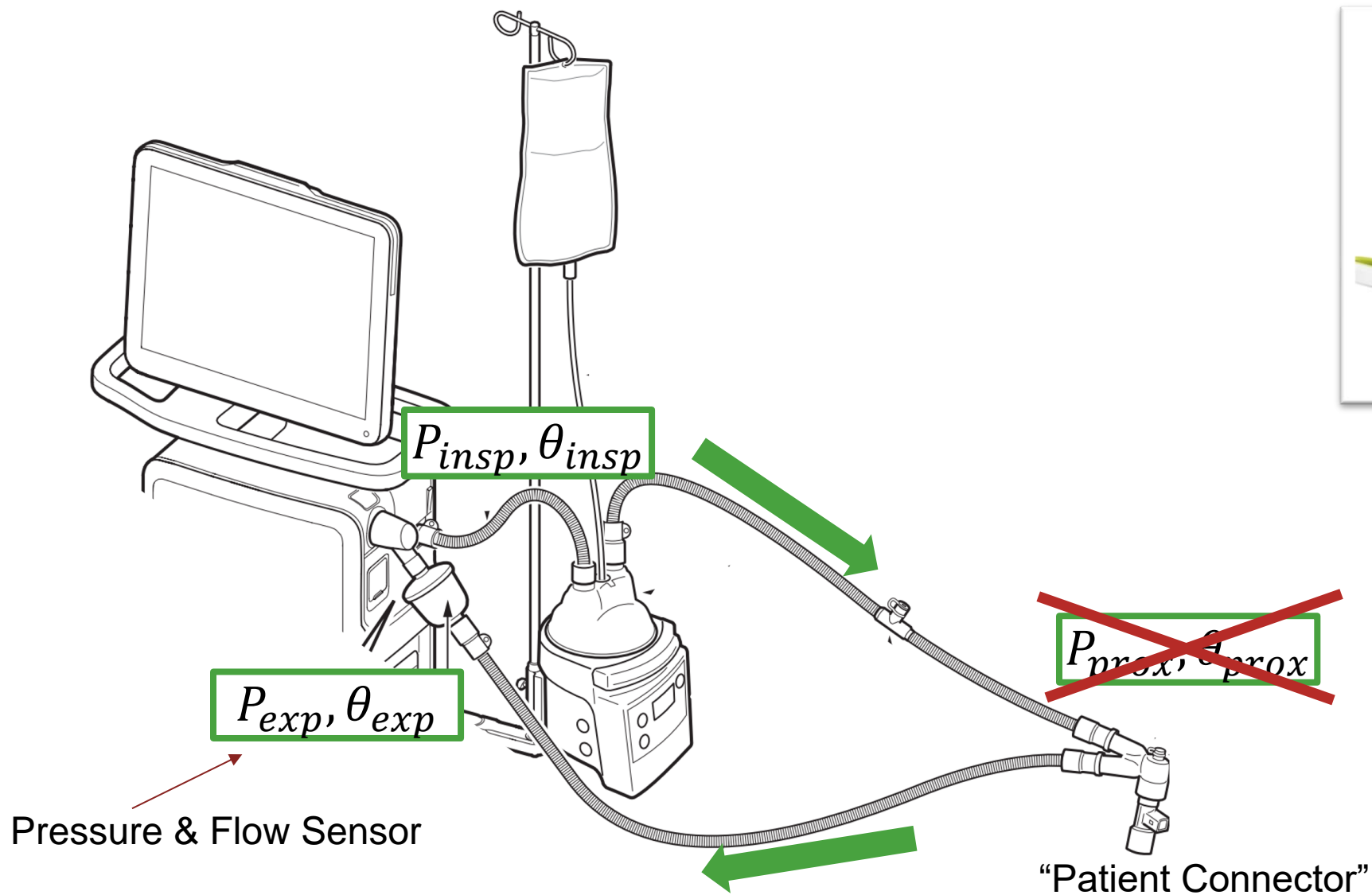




# Getinge



# The mechanical Ventilator – What could go wrong?



## Risk Management vs FMEA

Risk Management (ISO 14971)	FMEA (IEC 60812)
<b>Normal</b> and fault condition	<b>Only</b> fault condition
Starts with <b>Hazard</b>	Starts with detailed components
Severity based on <b>Patient</b>	Severity based on <b>system performance</b>
Manage all risks	Improve <b>reliability</b>



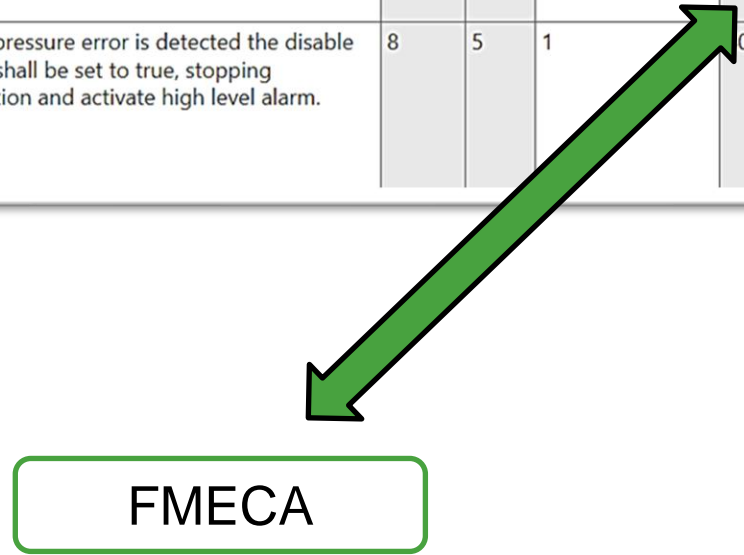
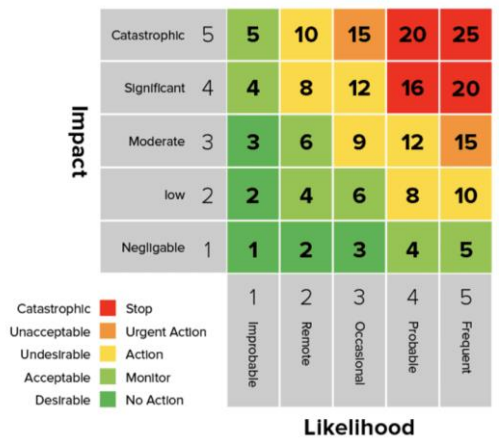
## Risk Management vs FMEA

Risk Management (ISO 14971)	FMEA (IEC 60812)
<b>Normal</b> and fault condition	<b>Only</b> fault condition
Starts with <b>Hazard</b>	Starts with detailed components
Severity based on <b>Patient</b>	Severity based on <b>system performance</b>
Manage all risks	Improve <b>reliability</b>

# FMEA (IEC 60812)


Automated FMEA for a ventilator Extended X

	System	Function	Failure	Local Effect	System Effect	S	Po	Detection	RPN	Detection/MOC	MOC req ref	S	O	D after MOC	RPN after ...
1	Sensors	Proximal Pressure Sensor	Incorrect value	Incorrect pressure control. Higher true pressure if control pressure is falsly lower.	Possible barotrauma.	8	8	10	640	Pressure Error Detection using Proximal pressure sensor estimation	When pressure error is detected the disable valves shall be set to true, stopping ventilation and activate high level alarm.	8	8	1	64
2	Sensors	Insp Pressure Sensor	Incorrect value	Incorrect pressure control. Higher true pressure if control pressure is falsly lower.	Possible barotrauma.	8	5	10	400	Pressure Error Detection using Proximal pressure sensor estimation	When pressure error is detected the disable valves shall be set to true, stopping ventilation and activate high level alarm.	8	5	1	40
3	Sensors	Exp Pressure Sensor	Incorrect value	Incorrect pressure control. Higher true pressure if control pressure is falsly lower.	Possible barotrauma.	8	5	10	400	Pressure Error Detection using Proximal pressure sensor estimation	When pressure error is detected the disable valves shall be set to true, stopping ventilation and activate high level alarm.	8	5	1	40




# Typical FMEA work

Automated FMEA for a ventilator Extended X

	⌘ Syst...	⌘ Function	⌘ Failure	⌘ Local Effect	⌘ System Effect	⌘ S	⌘ Po	⌘ Detection	⌘ RPN
1	Sensors	Proximal Pressure Sensor	Incorrect value 	Incorrect pressure control. Higher true pressure if control pressure is falsly lower.	Possible barotrauma.	8	8	10	640


# Typical FMEA work

Automated FMEA for a ventilator Extended X

	⌘ Syst...	⌘ Function	⌘ Failure	⌘ Local Effect	⌘ System Effect	⌘ S	⌘ Po	⌘ Detection	⌘ RPN
1	Sensors	Proximal Pressure Sensor	Incorrect value 	Incorrect pressure control. Higher true pressure if control pressure is falsly lower.	Possible barotrauma.	8	8	10	640

# Typical FMEA work

Automated FMEA for a ventilator Extended X

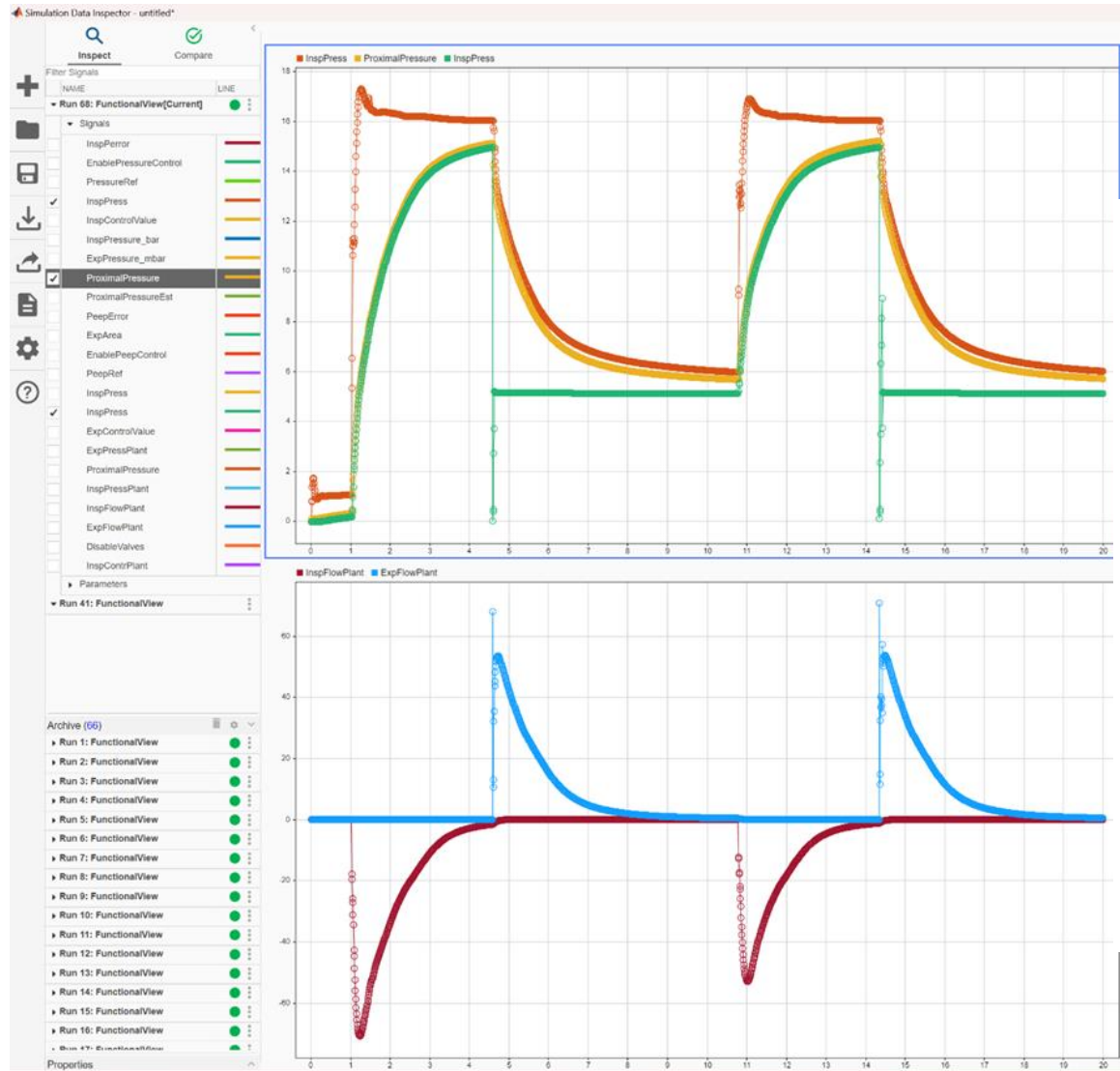
	⌘ Syst...	⌘ Function	⌘ Failure	⌘ Local Effect	⌘ System Effect	⌘ S	⌘ Po	⌘ Detection	⌘ RPN
1	Sensors	Proximal Pressure Sensor	Incorrect value 	Incorrect pressure control. Higher true pressure if control pressure is falsly lower.	Possible barotrauma.	8	8	10	640

$$\text{RPN} = \text{S} * \text{Po} * \text{Detection} = 8 * 8 * 10 = 640$$

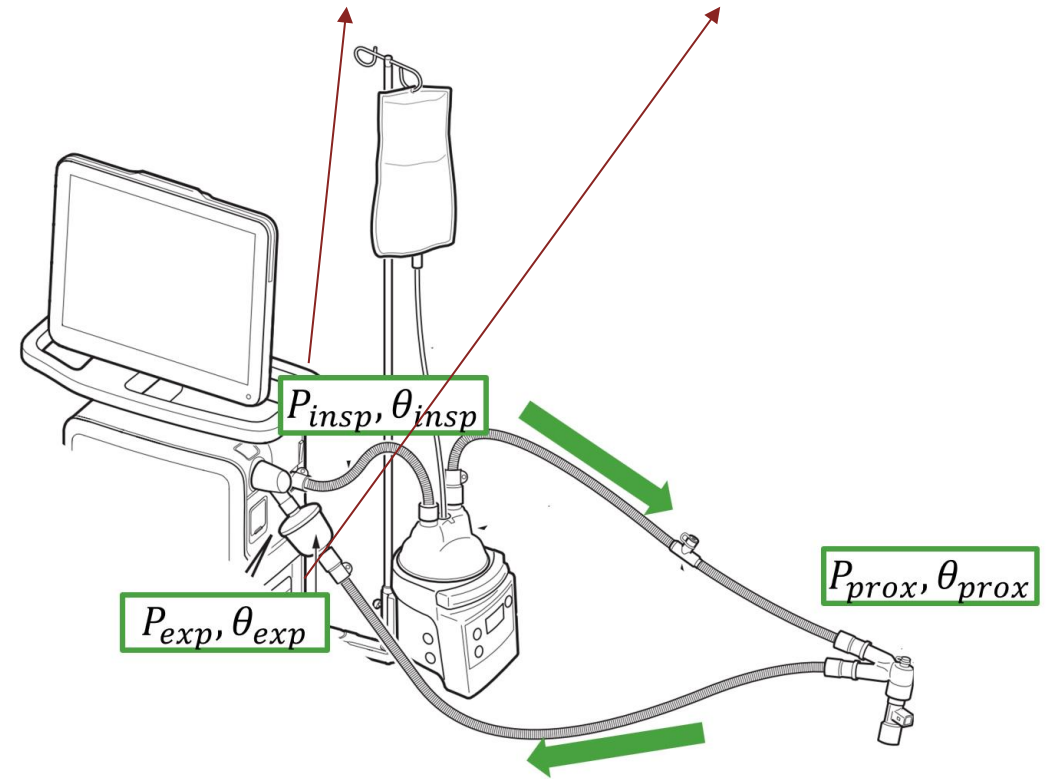
Risk Priority Number



# The mechanical Ventilator – redundancy.



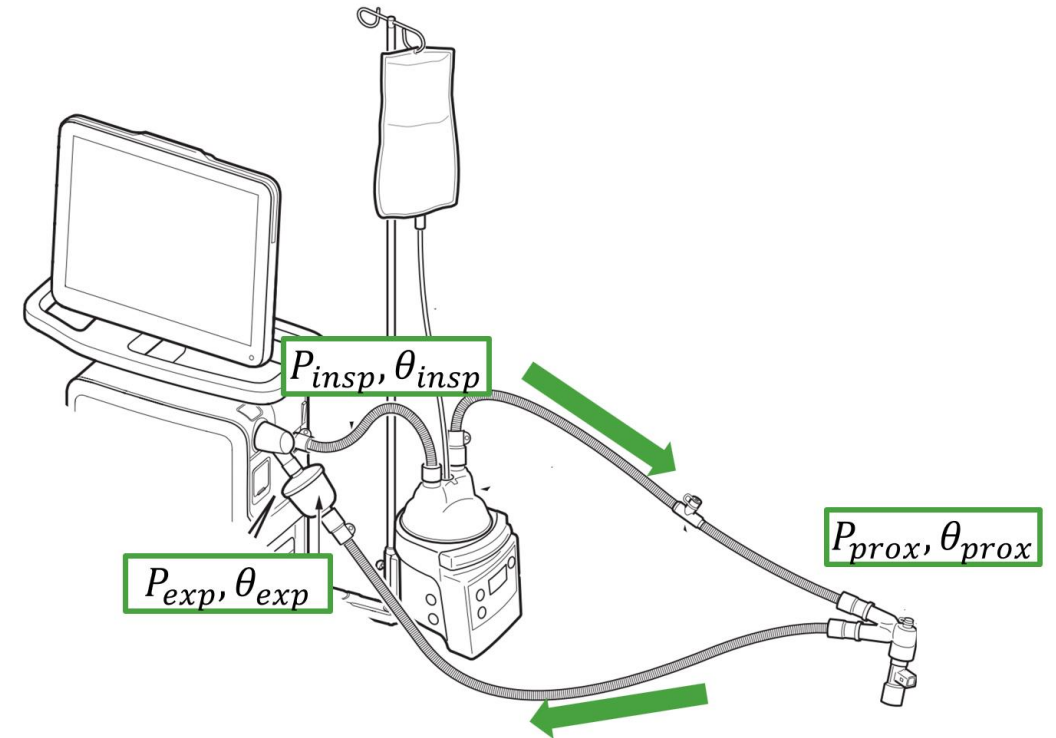
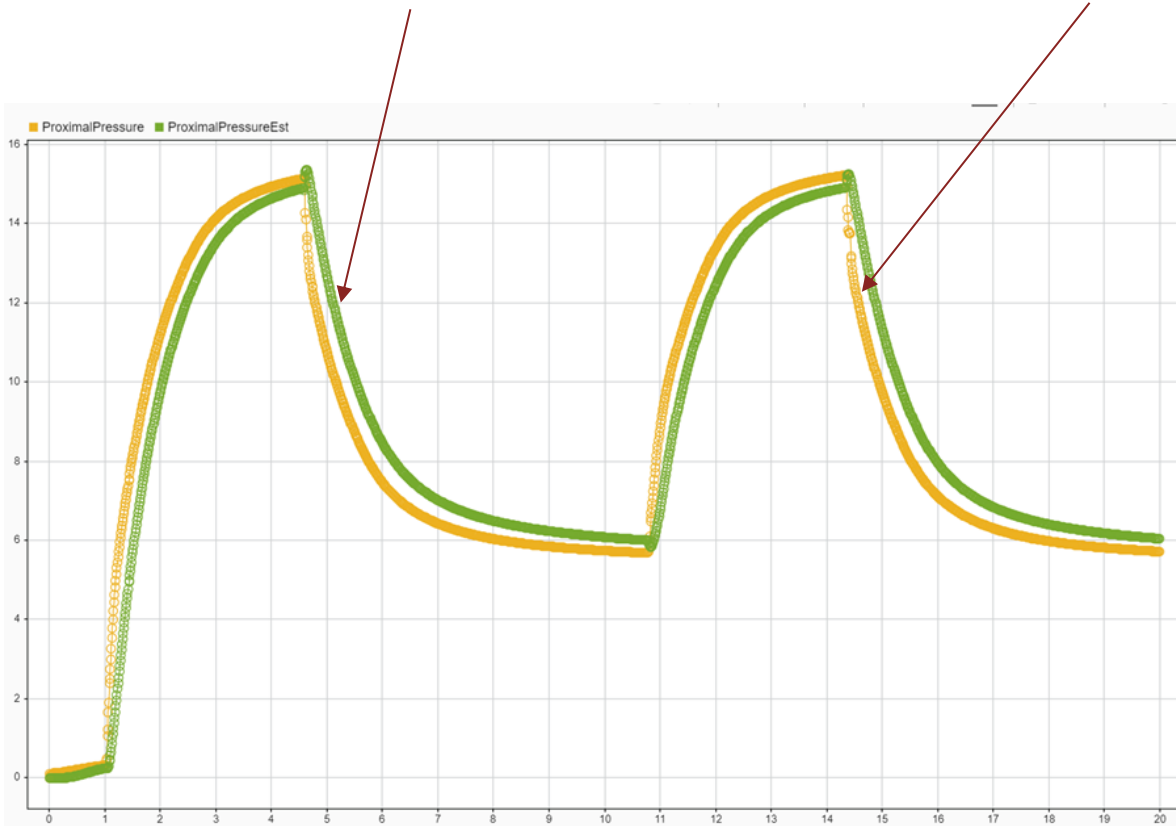
$$\hat{P}_{prox} = f(P_{insp}, \theta_{insp}, P_{exp}, \theta_{exp})$$







# The mechanical Ventilator – redundancy.

$$\hat{P}_{prox} = f(P_{insp}, \theta_{insp}, P_{exp}, \theta_{exp}) \quad P_{prox}$$



## Typical FMEA work



⌵ RPN	⌵ Detection/MOC	⌵ MOC req ref	⌵ S	⌵ O	⌵ D after MOC	⌵ RPN after ...
640	Pressure Error Detection using Proximal pressure sensor estimation   	When pressure error is detected the disable valves shall be set to true, stopping ventilation and activate high level alarm.	8	8	1	64

MOC = Method Of Control

## Typical FMEA work

⌵ RPN	⌵ Detection/MOC	⌵ MOC req ref	⌵ S	⌵ O	⌵ D after MOC	⌵ RPN after ...
640	Pressure Error Detection using Proximal pressure sensor estimation  ✔️🔗	When pressure error is detected the disable valves shall be set to true, stopping ventilation and activate high level alarm.	8	8	1	64

## Typical FMEA work

⌵ RPN	⌵ Detection/MOC	⌵ MOC req ref	⌵ S	⌵ O	⌵ D after MOC	⌵ RPN after ...
640	Pressure Error Detection using Proximal pressure sensor estimation   	When pressure error is detected the disable valves shall be set to true, stopping ventilation and activate high level alarm.	8	8	1	64










# Typical FMEA work

⌘ RPN	⌘ Detection/MOC	⌘ MOC req ref	⌘ S	⌘ O	⌘ D after MOC	⌘ RPN after ...
640	Pressure Error Detection using Proximal pressure sensor estimation  ✔️🔗	When pressure error is detected the disable valves shall be set to true, stopping ventilation and activate high level alarm.	8	8	1	64

$$\text{RPN} = \text{S} * \text{Po} * \text{Detection} = 8 * 8 * 1 = 64$$

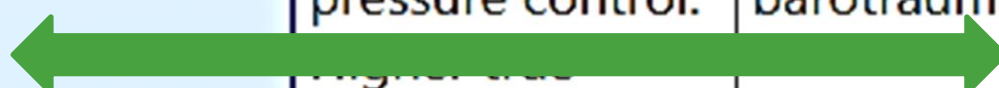
# Typical FMEA work

Where are the problems with a manual workflow?

Automated FMEA for a ventilator Extended X															
	⌘ Syst...	⌘ Function	⌘ Failure	⌘ Local Effect	⌘ System Effect	⌘ S	⌘ Po	⌘ Detection	⌘ RPN	⌘ Detection/MOC	⌘ MOC req ref	⌘ S	⌘ O	⌘ D after MOC	⌘ RPN after ...
1	Sensors	Proximal Pressure Sensor	Incorrect value 	Incorrect pressure control. Higher true pressure if control pressure is falsly lower.	Possible barotrauma.	8	8	10	640	Pressure Error Detection using Proximal pressure sensor estimation  	When pressure error is detected the disable valves shall be set to true, stopping ventilation and activate high level alarm.	8	8	1	64
2	Sensors	Insp Pressure Sensor	Incorrect value 	Incorrect pressure control. Higher true pressure if control pressure is falsly lower.	Possible barotrauma.	8	5	10	400	Pressure Error Detection using Proximal pressure sensor estimation  	When pressure error is detected the disable valves shall be set to true, stopping ventilation and activate high level alarm.	8	5	1	40
3	Sensors	Exp Pressure Sensor	Incorrect value 	Incorrect pressure control. Higher true pressure if control pressure is falsly lower.	Possible barotrauma.	8	5	10	400	Pressure Error Detection using Proximal pressure sensor estimation  	When pressure error is detected the disable valves shall be set to true, stopping ventilation and activate high level alarm.	8	5	1	40



## Typical FMEA work

for Extended X					
	:: Failure	:: Local Effect	:: System Effect	:: S	:: Po
ure	Incorrect value	Incorrect pressure control.	Possible barotrauma.	8	8
		Higher than control pressure if control pressure is falsly lower.			

Complicated cause and effect reasoning

# Typical FMEA work

	Failure	Local Effect	System Effect	S	Po	Detection	RPN	Detection/MOC	MOC req ref
Pressure	Incorrect value	Incorrect pressure control. Higher true pressure if control pressure is falsly lower.	Possible barotrauma.	8	8	10	640	Pressure Error Detection using Proximal pressure sensor estimation	When pressure error valves shall be set to ventilation and activation

Complicated cause and effect reasoning

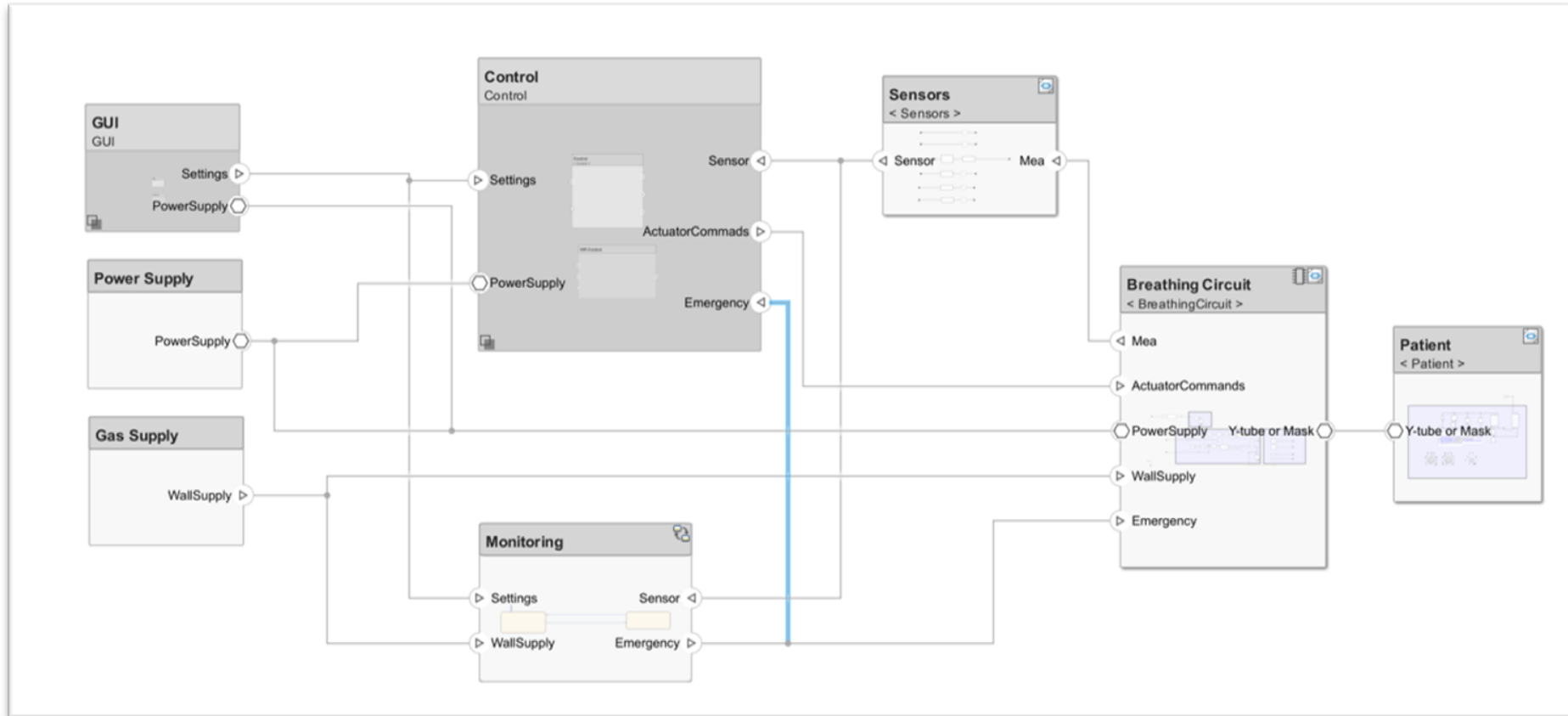
Is the MOC really solving the problem?

Manual labour

Error prone

What if you could...

Manage the system level design and....



# What if you could...

## Automate the FMEA MOC verification...

Safety Analysis Manager

HOME

FILE EDIT SPREADSHEET LINKS SEARCH ANALYZE SHARE

Open Save Import Paste Copy Delete Add Row Add Column View Columns Add Link Find Analyze Spreadsheet Edit Callbacks Clear Flags Export

Automated FMEA for a ventilator\* X

System/Subsystem	Function	Failure	Severity	Occurance	Detection	RPN	Detection/MOC	MOC req ref	S	O	D after MOC	RPN after ...
Sensors	Proximal Pressure Sensor	Incorrect value	10	10	10	1000	Pressure Error Detection using Proximal pressure sensor estimation ✔️🔗	Link to requirement	10	10	1	100
Sensors	Insp Pressure Sensor	Incorrect value	10	5	10	500	Pressure Error Detection using Proximal pressure sensor estimation ✔️🔗	Link to requirement	10	5	1	50
Sensors	Exp Pressure Sensor	Incorrect value	10	5	10	500	Pressure Error Detection using Proximal pressure sensor estimation ✔️🔗	Link to requirement	10	5	1	50

# What if you could...

## Safeguard the digital thread throughout the project...

Safety Analysis Manager

HOME

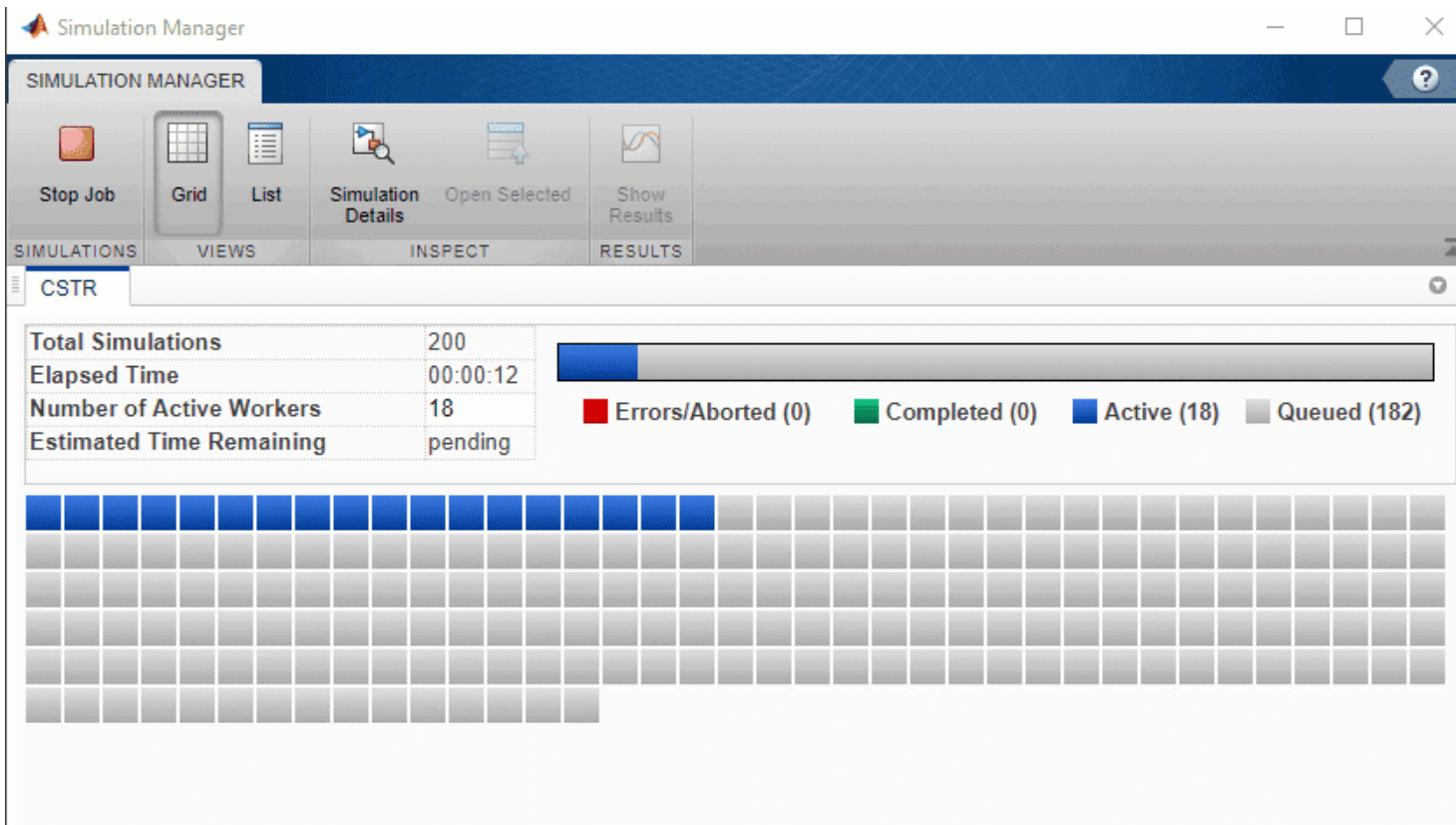
FILE EDIT SPREADSHEET LINKS SEARCH ANALYZE SHARE

Automated FMEA for a ventilator\* X

System/Subsystem	Function	Failure	Severity	Occurance	Detection	RPN	Detection/MOC	MOC req ref	S	O	D after MOC	RPN after ...
Sensors	Proximal Pressure Sensor	Incorrect value <a href="#">🔗</a>	10	10	10	1000	Pressure Error Detection using Proximal pressure sensor estimation <input checked="" type="checkbox"/> <a href="#">🔗</a>	Link to requirement <a href="#">🔗</a>	10	10	1	100
Sensors	Insp Pressure Sensor	Incorrect value <a href="#">🔗</a>	10	5	10	500	Pressure Error Detection using Proximal pressure sensor estimation <input checked="" type="checkbox"/> <a href="#">🔗</a>	Link to requirement <a href="#">🔗</a>	10	5	1	50
Sensors	Exp Pressure Sensor	Incorrect value <a href="#">🔗</a>	10	5	10	500	Pressure Error Detection using Proximal pressure sensor estimation <input checked="" type="checkbox"/> <a href="#">🔗</a>	Link to requirement <a href="#">🔗</a>	10	5	1	50

# What if you could...

## Speed up extensive MOC validation ...



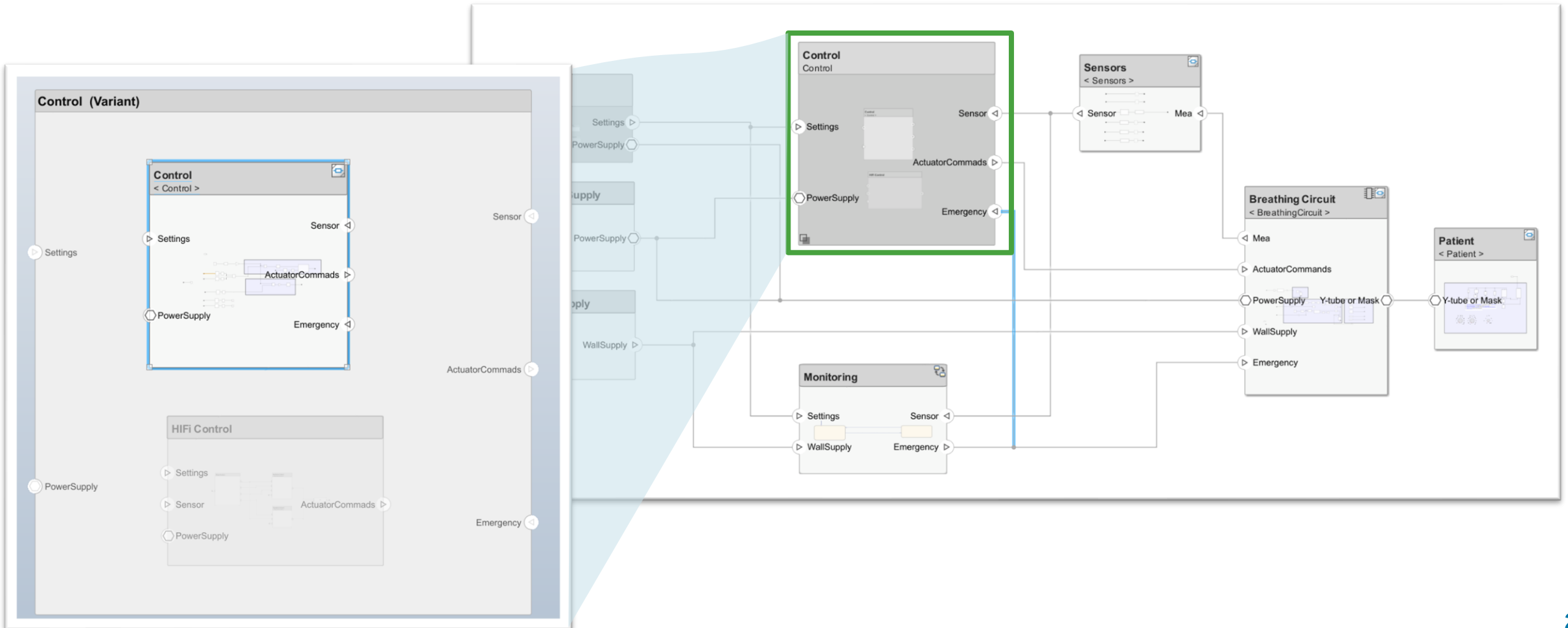
- Permutations on
- Pressure above Peep
  - Peep
  - Tidal Volume
  - I\_E ratio
  - Breath Rate
  - Patient Resistance
  - Patient Compliance

**10 000 to 100 000  
permutations**



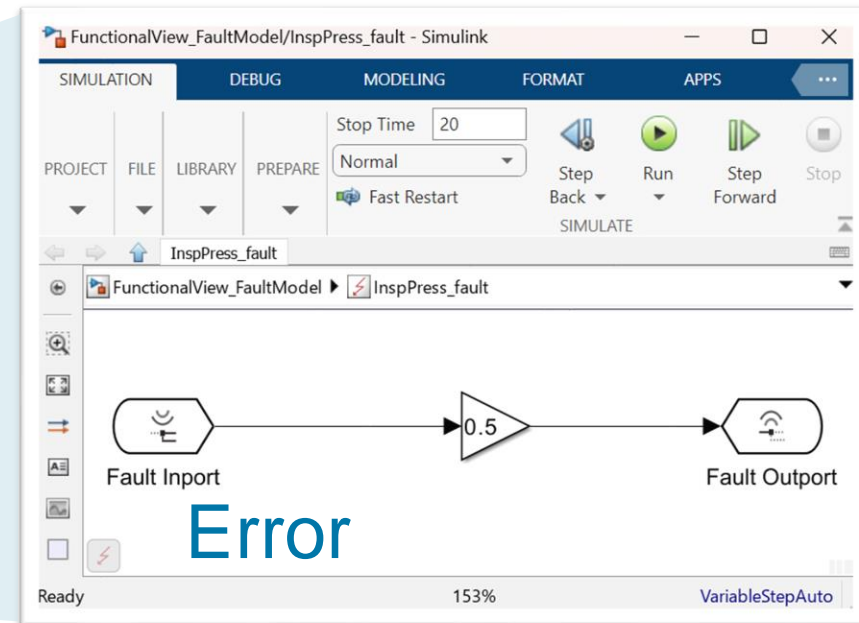
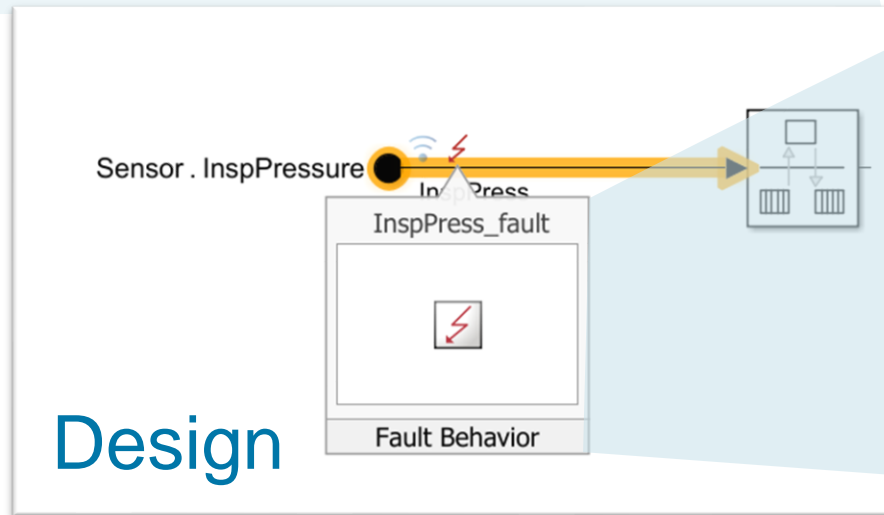
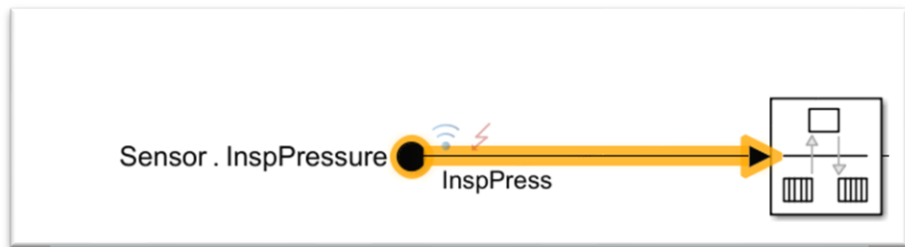
# What if you could...

## Ensure effective collaboration across your team....



# What if you could...

## Separate your design from your faults...



What if you could...

Have everything in reach using a model centric workflow...

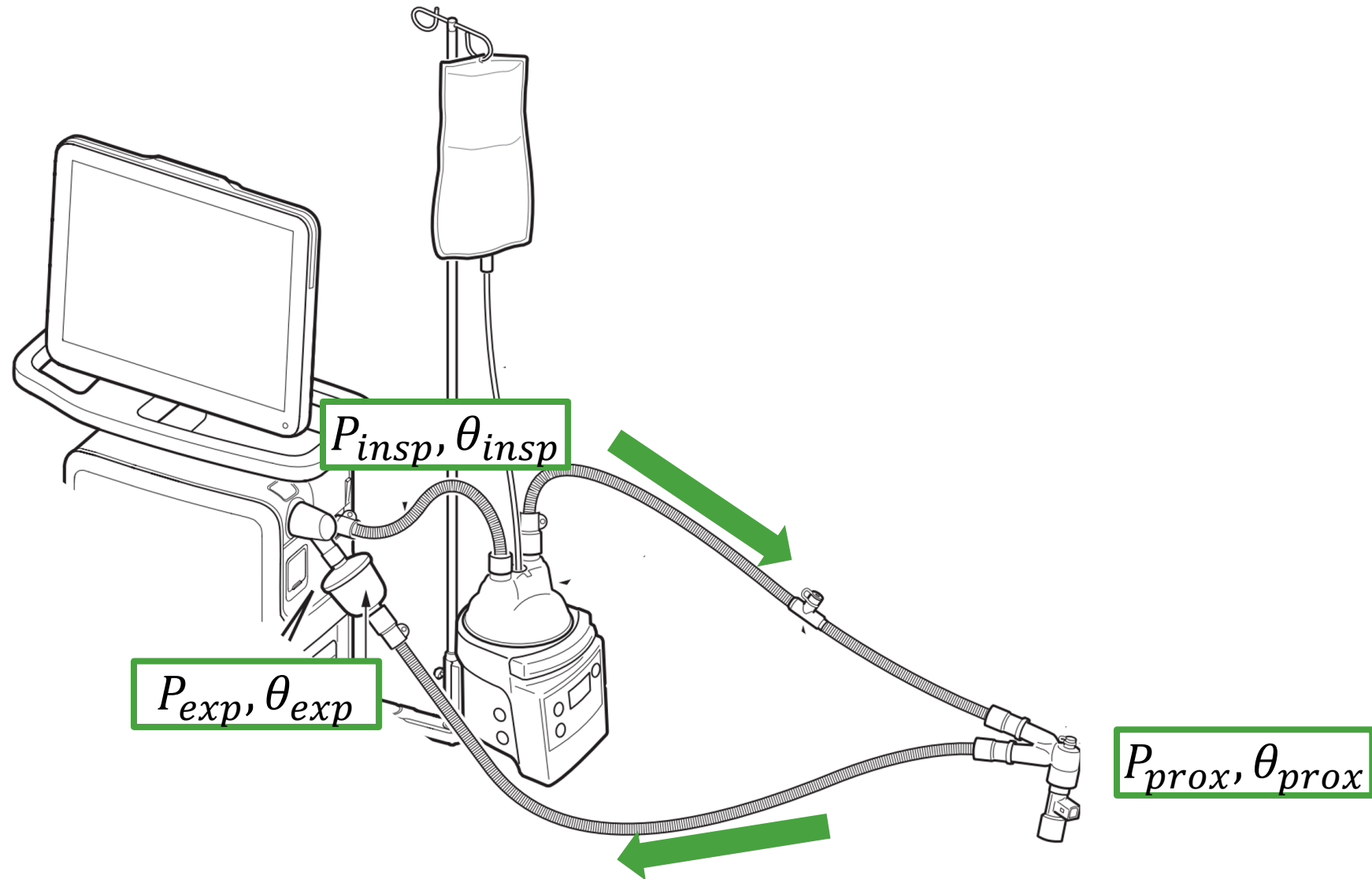
The screenshot displays the Simulink FunctionalView interface for a 'Breathing Circuit' model. The main workspace shows a block diagram with components like GUI, Power Supply, Gas Supply, Control, Sensors, Breathing Circuit, and Patient. Seven blue circles with numbers 1 through 7 are overlaid on the interface to highlight key features:

- 1**: Property Inspector showing details for Requirement #7.
- 2**: A requirement node in the model diagram.
- 3**: Requirements table listing various requirements.
- 4**: A requirement node in the model diagram with a red arrow pointing to its ID.
- 5**: Dictionary View showing a hierarchical list of model elements.
- 6**: Fault Table showing a table of faults.
- 7**: Links section in the Property Inspector showing implementation and verification links.

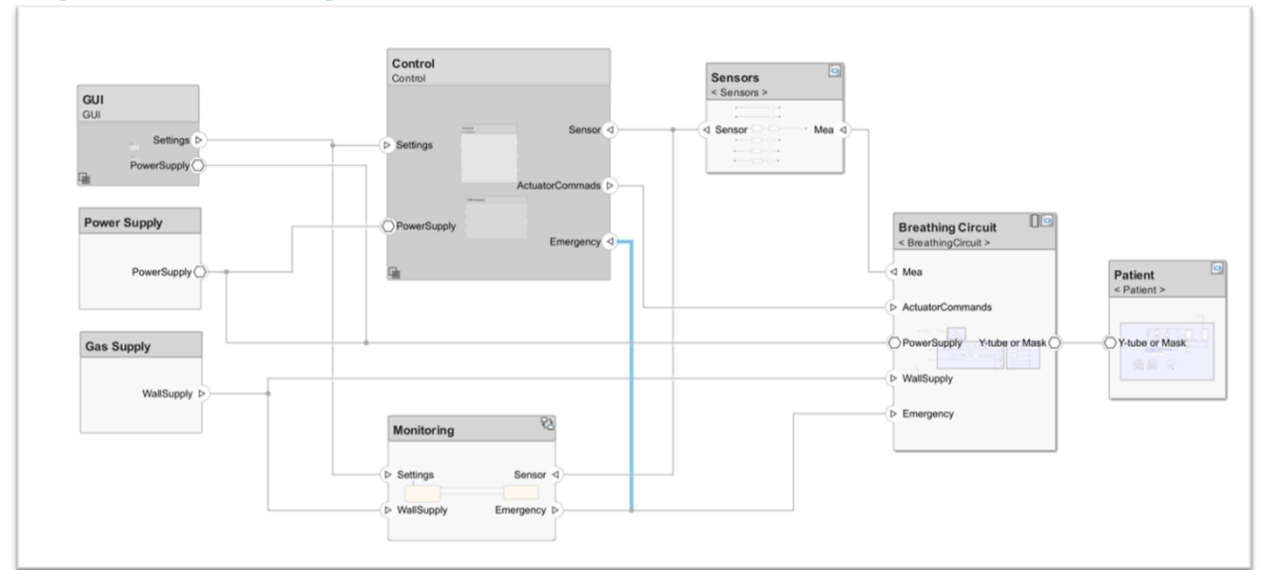
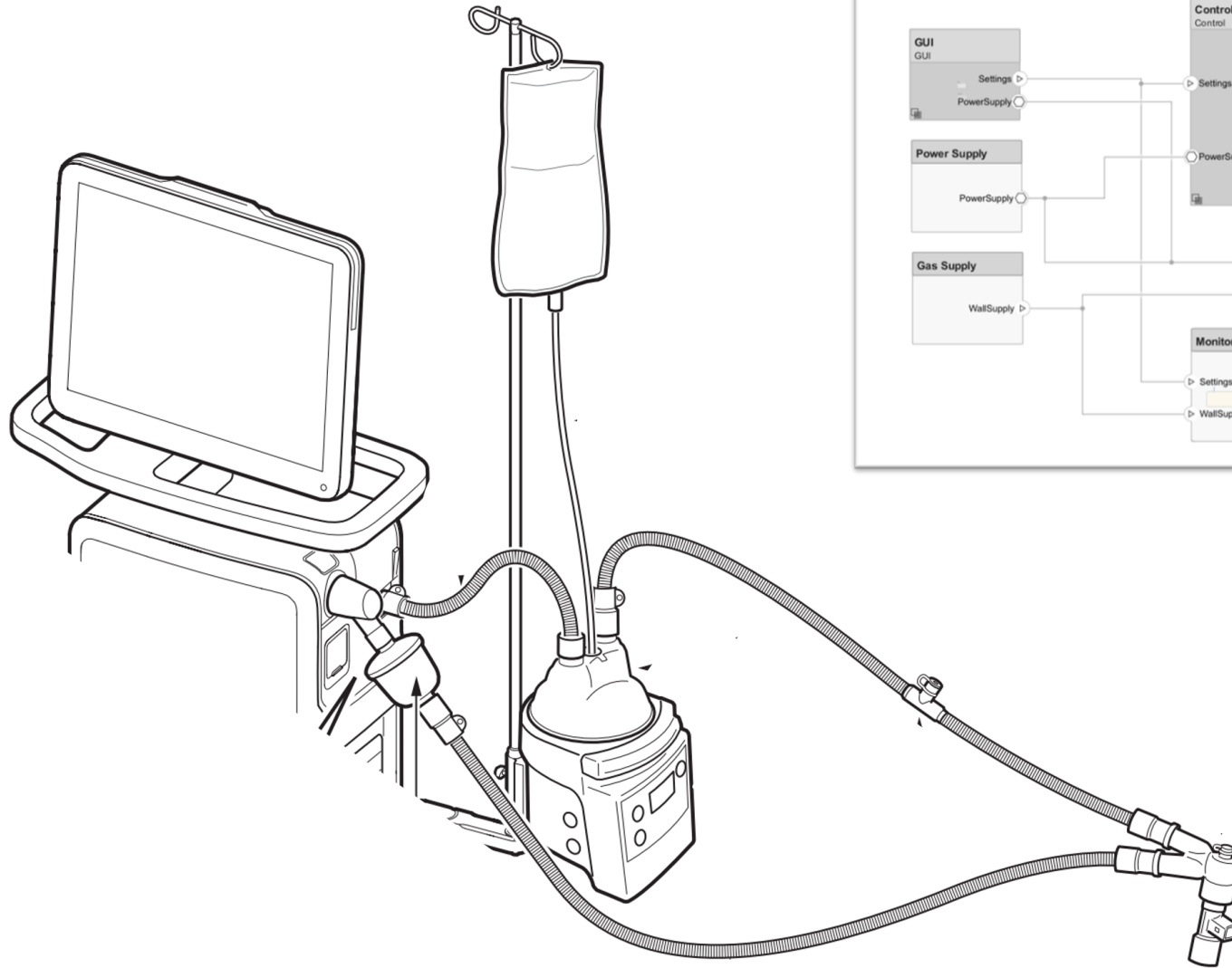
Index	ID	Description
1	#1	HighPressureAlarm
2	#7	TimeAtHighPressure
3	#3	HighPressureAlarmFor motion
4	#2	HighPressureEmergencyEvacuation
5	#6	PeakPressureDuringEvacuation
6	#4	The maximum pressure drop for emergency evacuation
7	#5	The HighPressureAlarmFor motion
8	#8	The system shall be able to reduce pressure using trap and

Enable	Model Element/Fau...	Active Fault	Trigger	Description
<input type="checkbox"/>	Control/Control...			

# The Mechanical Ventilator



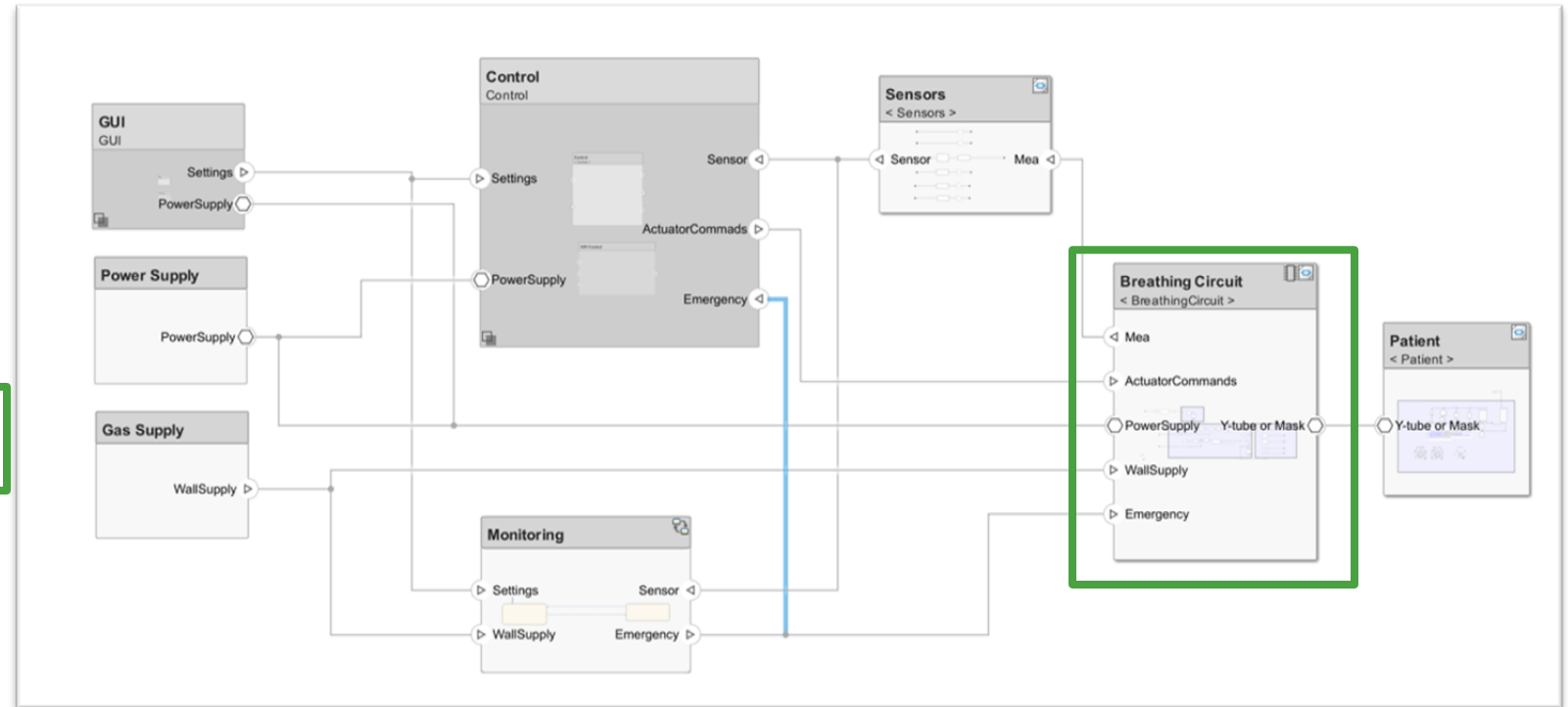
# Adding models to your System Engineering



# Adding models to your System Engineering

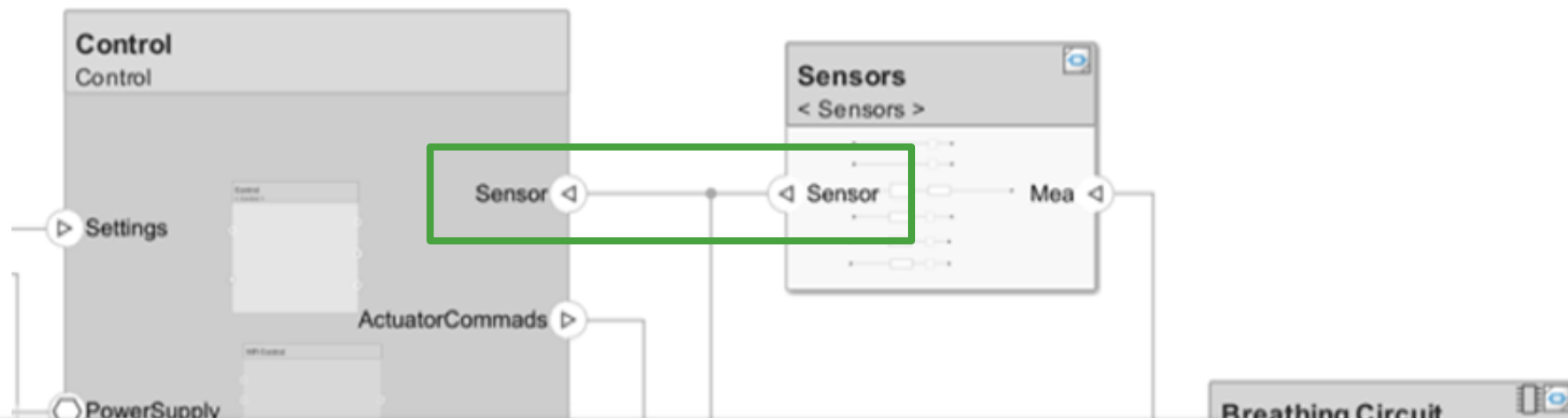
## Components

- GUI
- Control
- Monitoring
- Sensors
- Breathing Circuit
- Patient
- Power Supply
- Gas Supply





# Adding models to your System Engineering

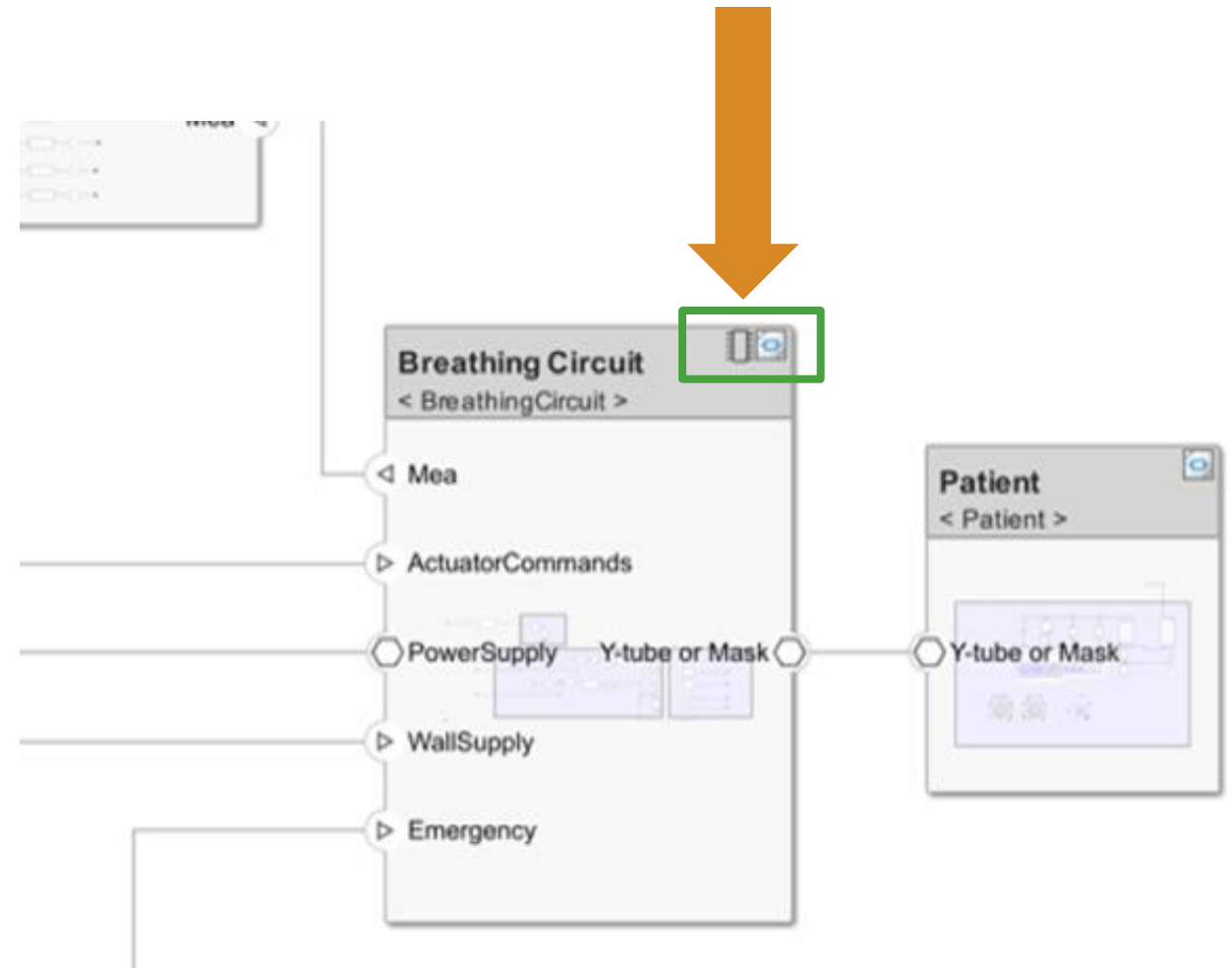


Sensor							
InspPressure	double	1	mbar	real	0	100	
ExpPressure	double	1	mbar	real	0	50	
InspFlow	double	1	l/min	real	0	180	
ExpFlow	double	1	l/min	real	0	300	
O2_Fraction	double	1	1	real	21	100	
ProximalPressure	double	1	mbar	real	[]	[]	
ProximalPressureEsstm:	double	1	mbar	real	[]	[]	

# Adding models to your System Engineering

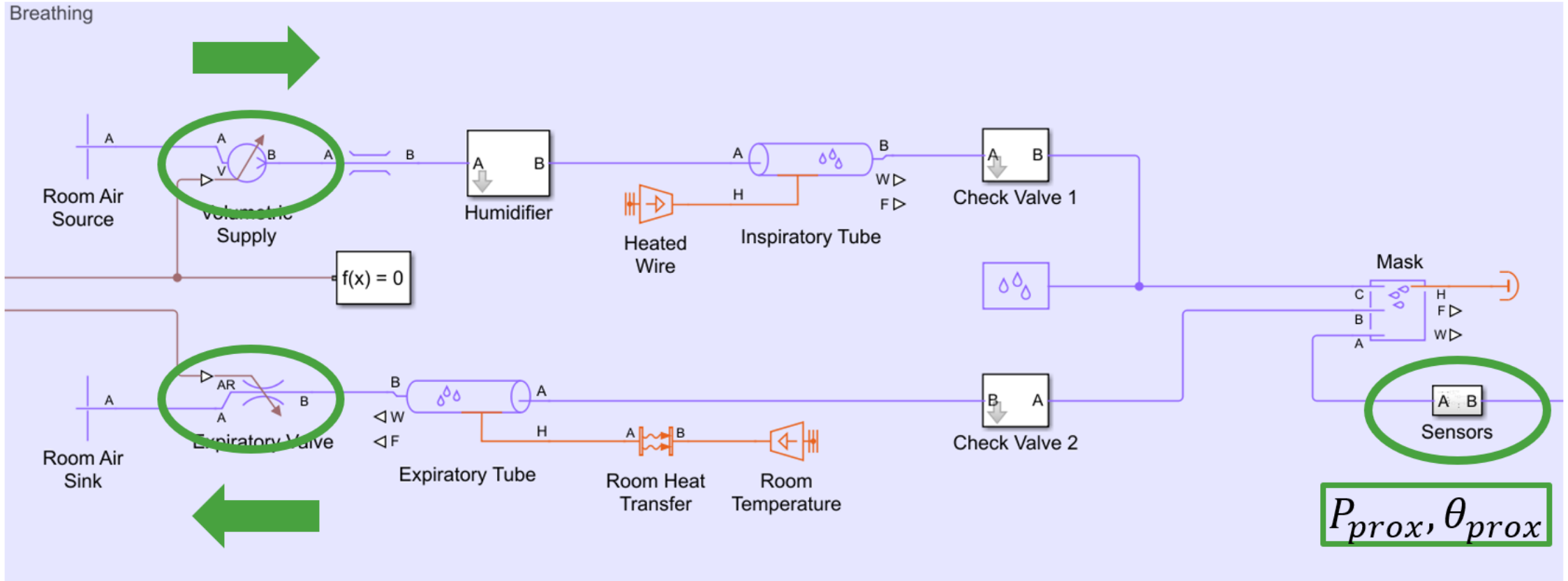
## Components

- GUI
- Control
- Monitoring
- Sensors
- **Breathing Circuit**
- Patient
- Power Supply
- Gas Supply



# Adding models to your System Engineering

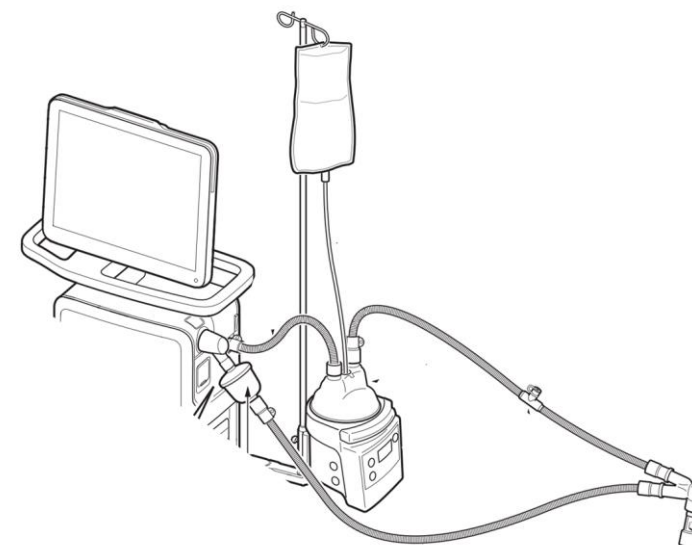
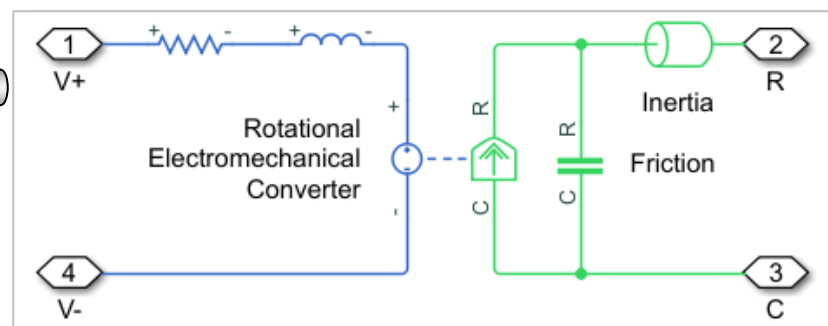
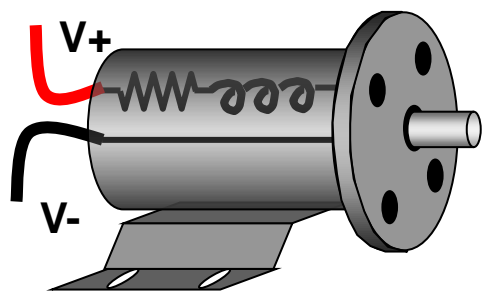
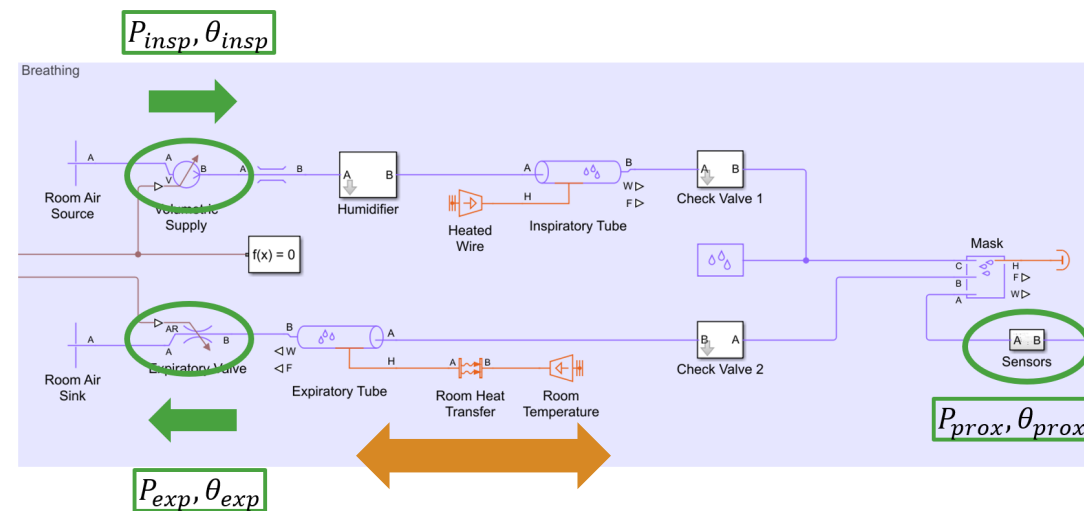
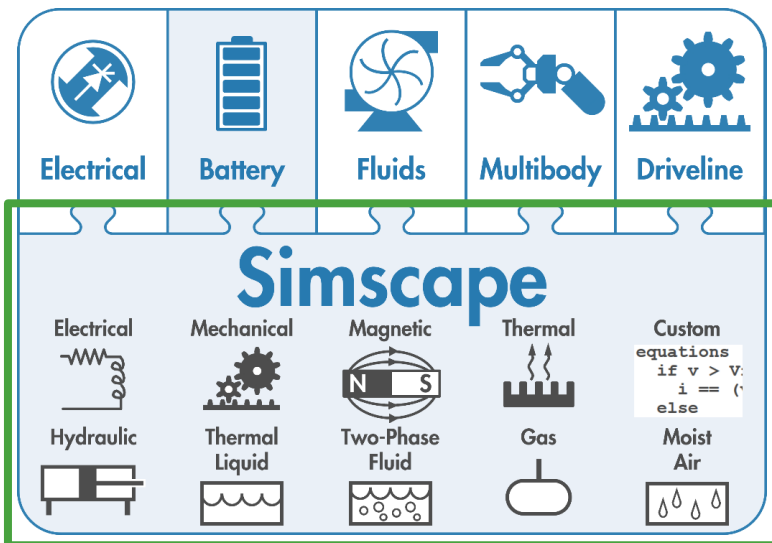
$P_{insp}, \theta_{insp}$








$P_{prox}, \theta_{prox}$

$P_{exp}, \theta_{exp}$







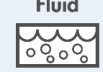


# Adding models to your System Engineering

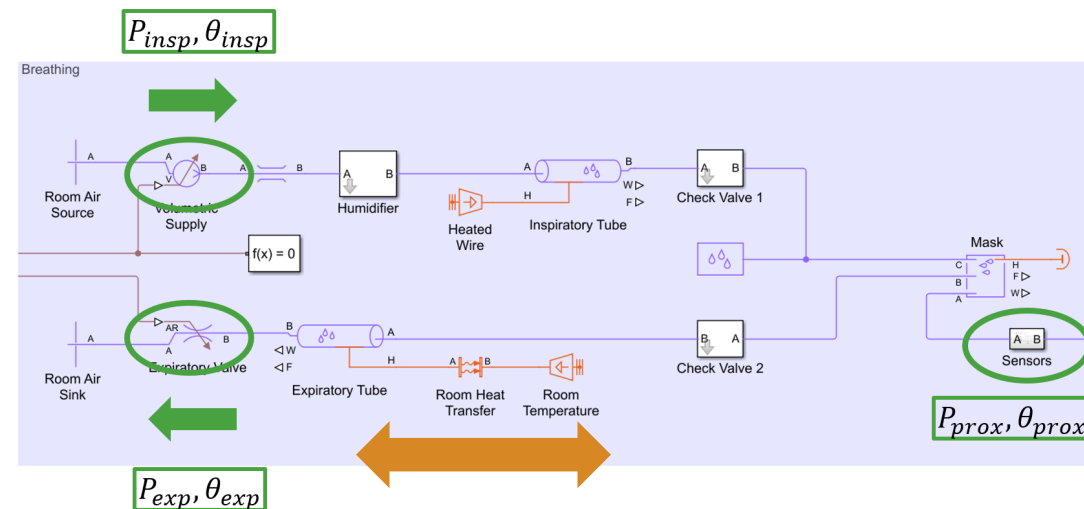


# Adding models to your System Engineering

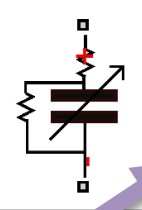
 Electrical	 Battery	 Fluids	 Multibody	 Driveline
---	--	---	--	--

## Simscape

Electrical 	Mechanical 	Magnetic 	Thermal 	Custom equations if v > v; i = (...) else
Hydraulic 	Thermal Liquid 	Two-Phase Fluid 	Gas 	Moist Air 



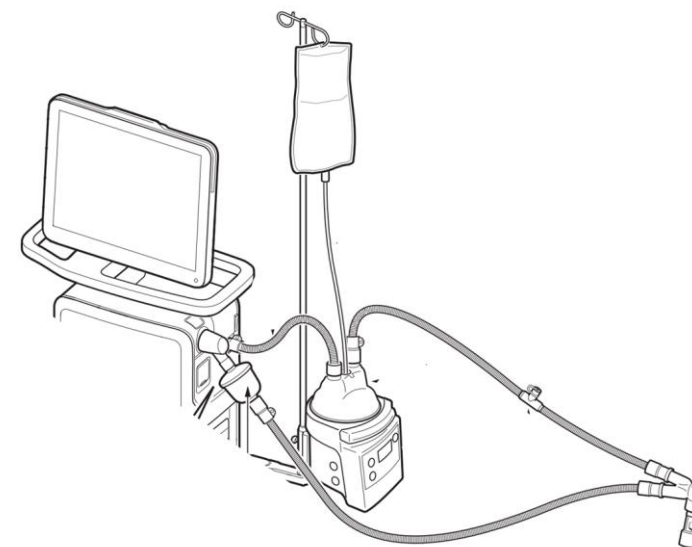
$$i = (C_0 + C_v v) \frac{dv}{dt} + \frac{v}{r_d}$$



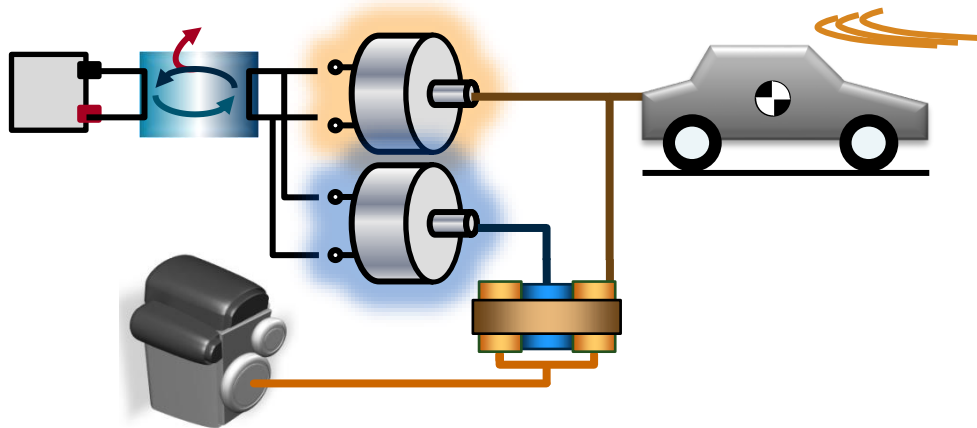
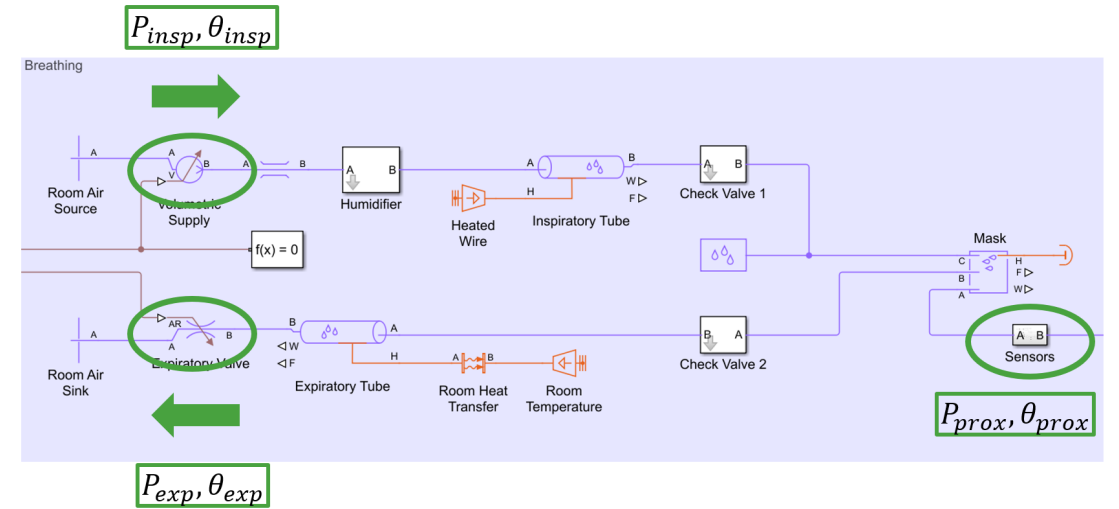
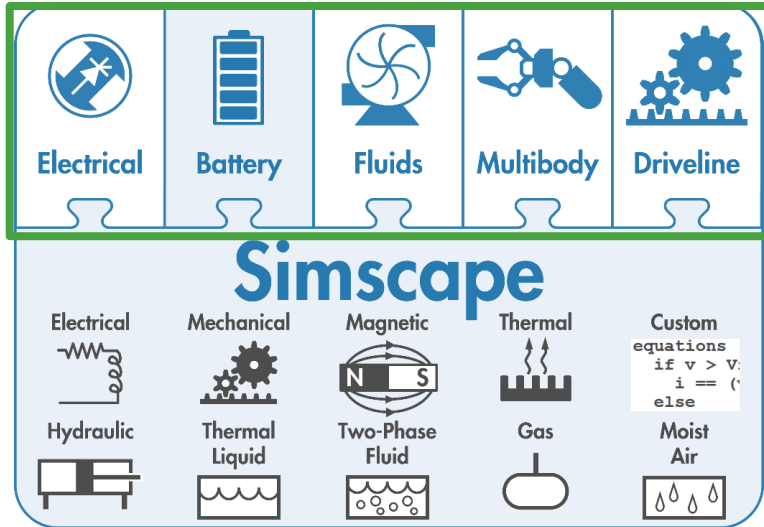
Lossy Ultracapacitor

```

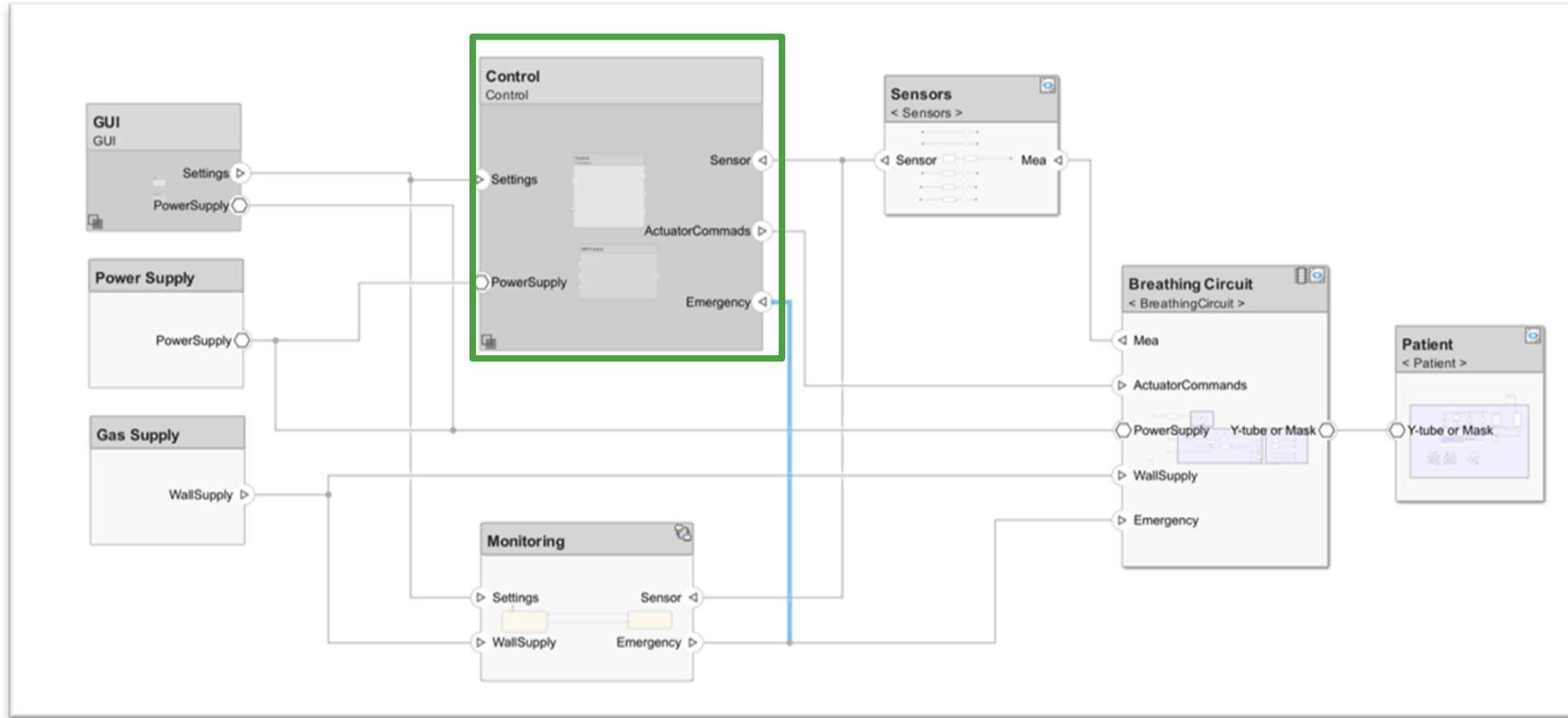
40 equations
41   i == (C0 + Cv*vc)*vc.der + vc/Rd;
42   v == vc + i*R;
43 end
    
```



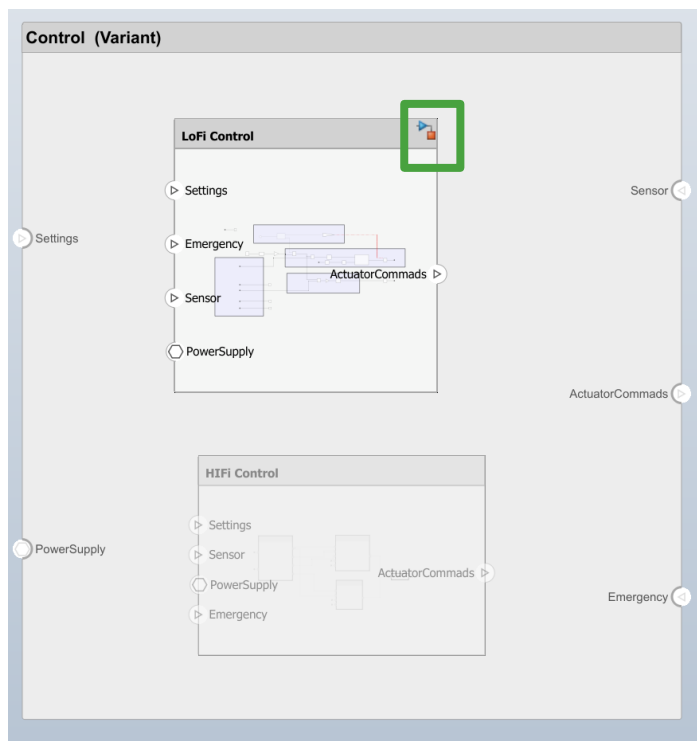
# Adding models to your System Engineering



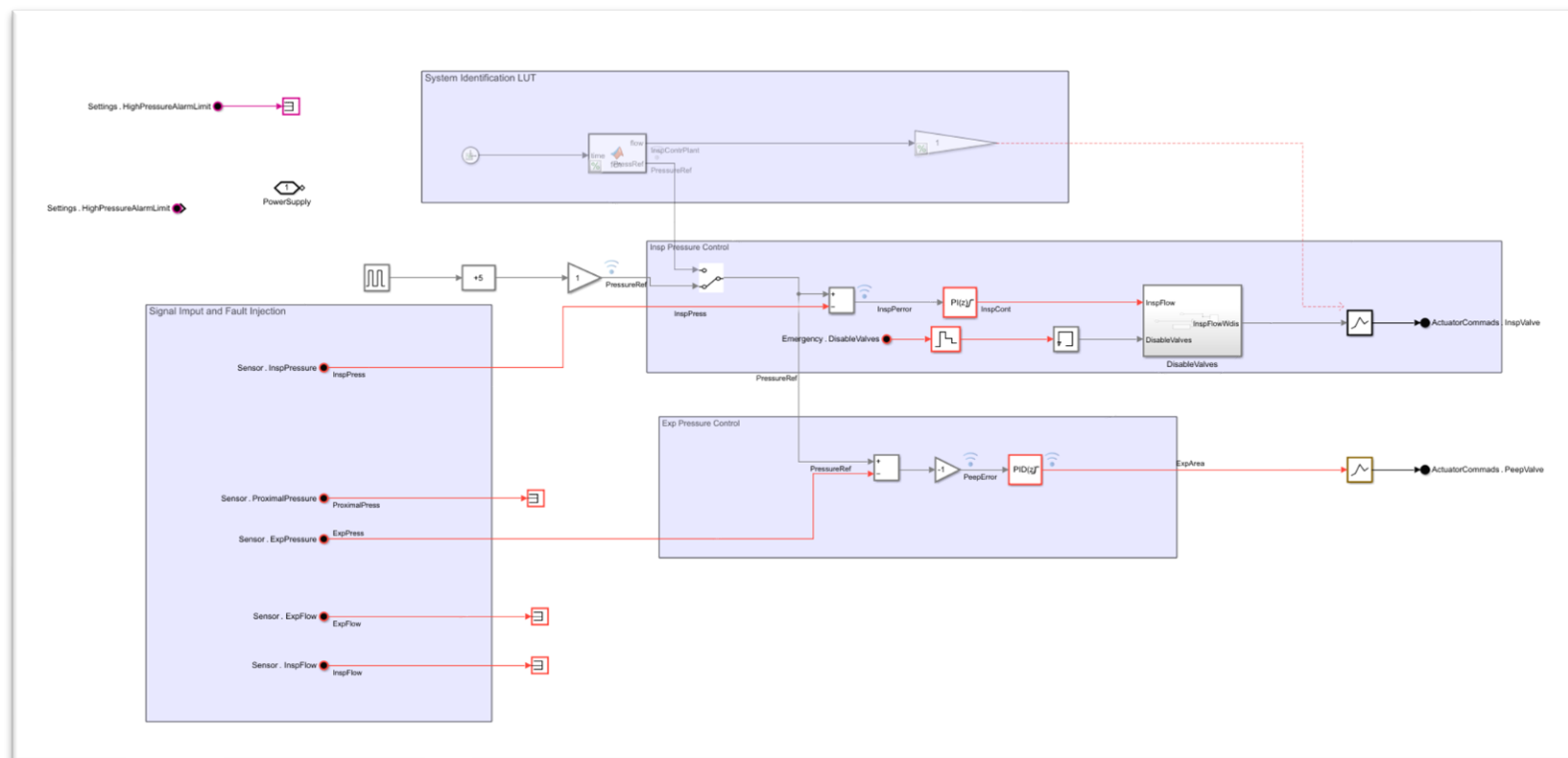
# Collaboration: System Engineer and Control Engineer



# Collaboration: System Engineer and Control Engineer

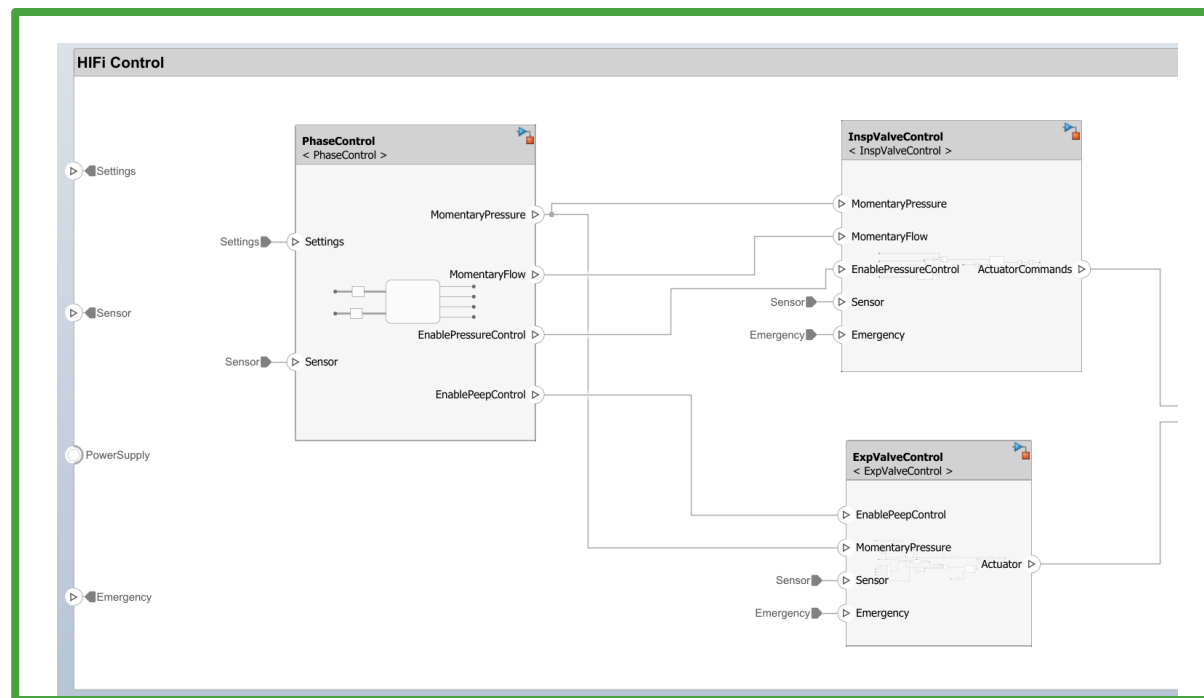
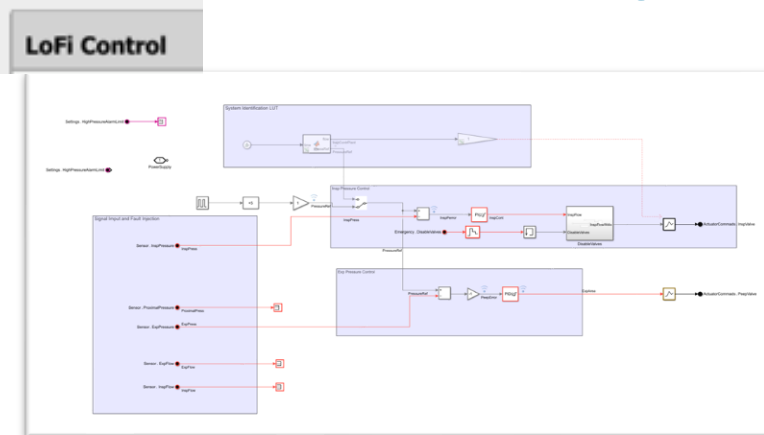
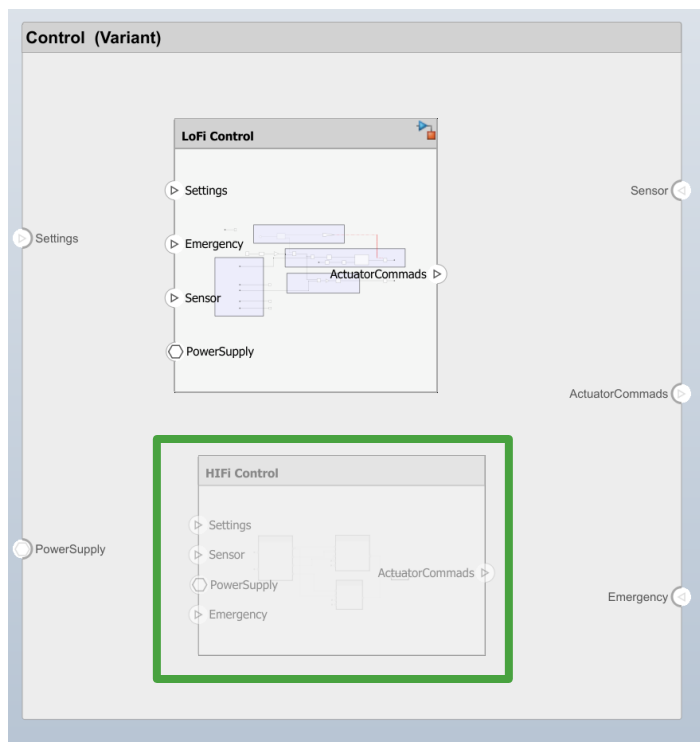


LoFi Control

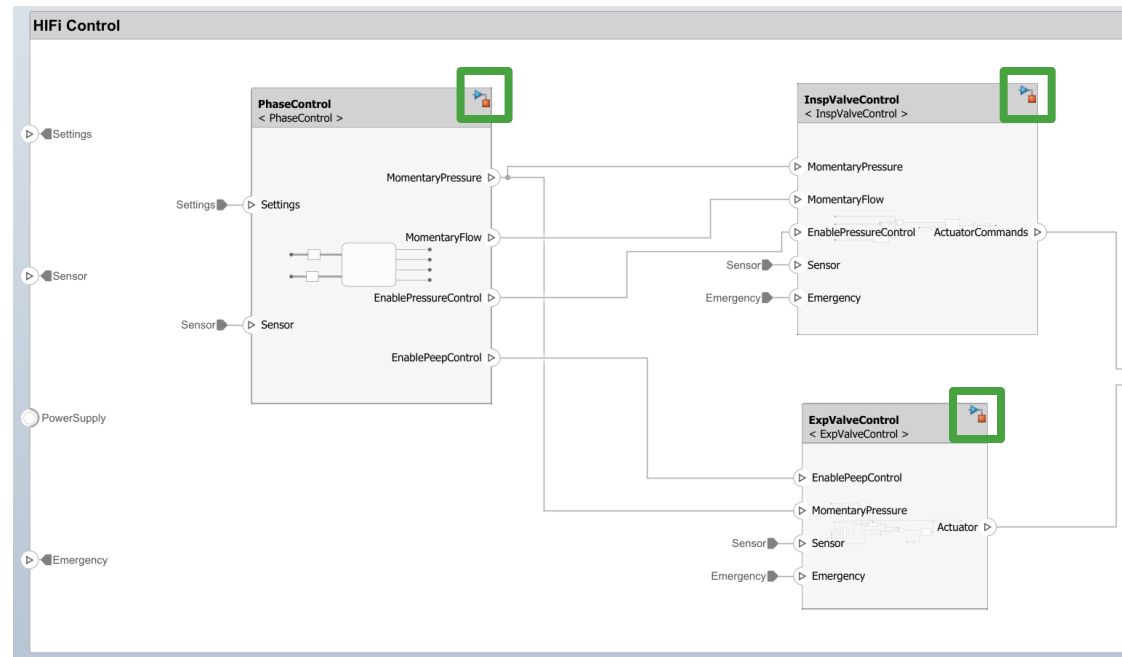
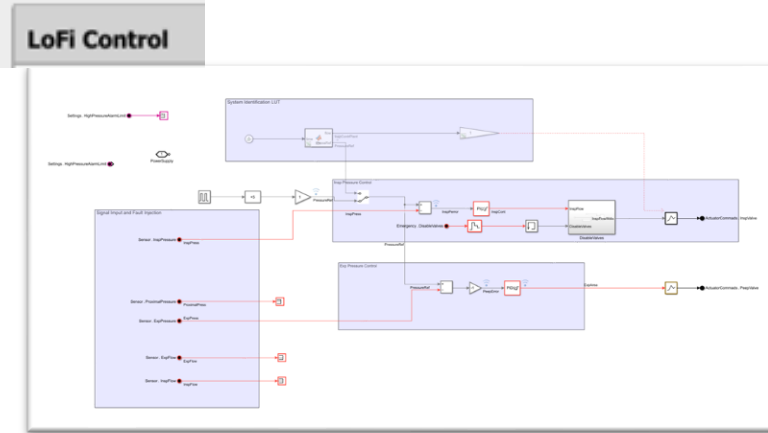
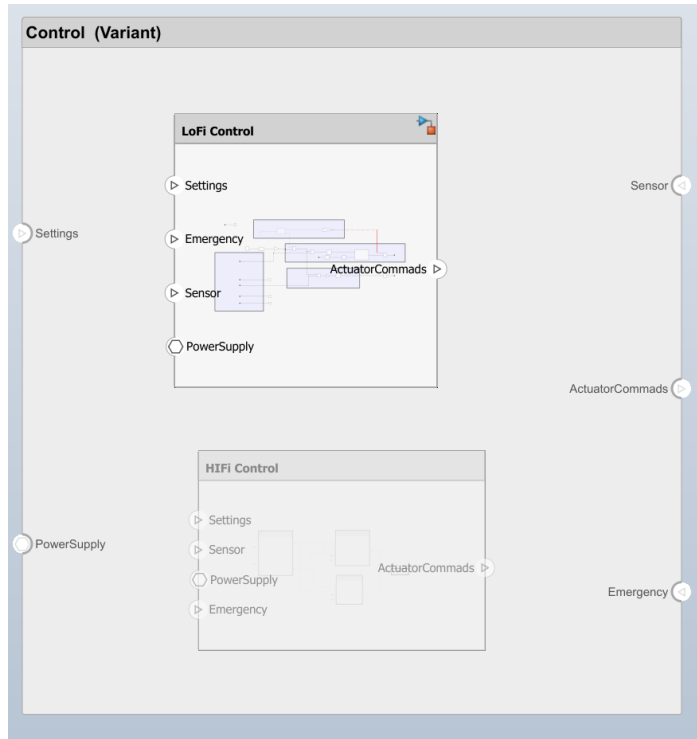




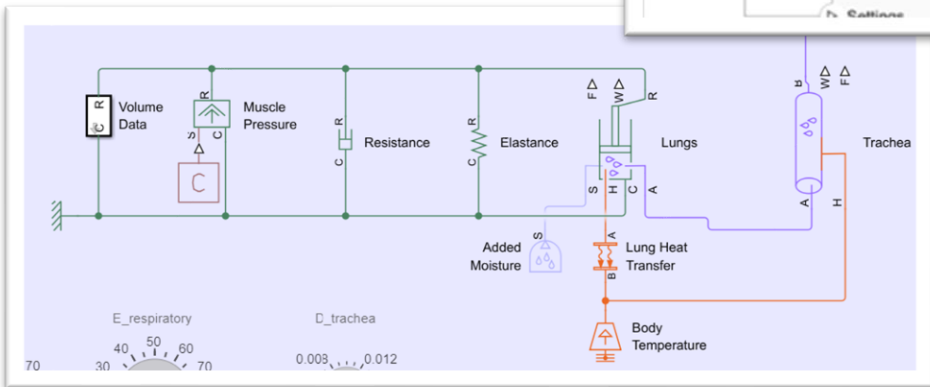
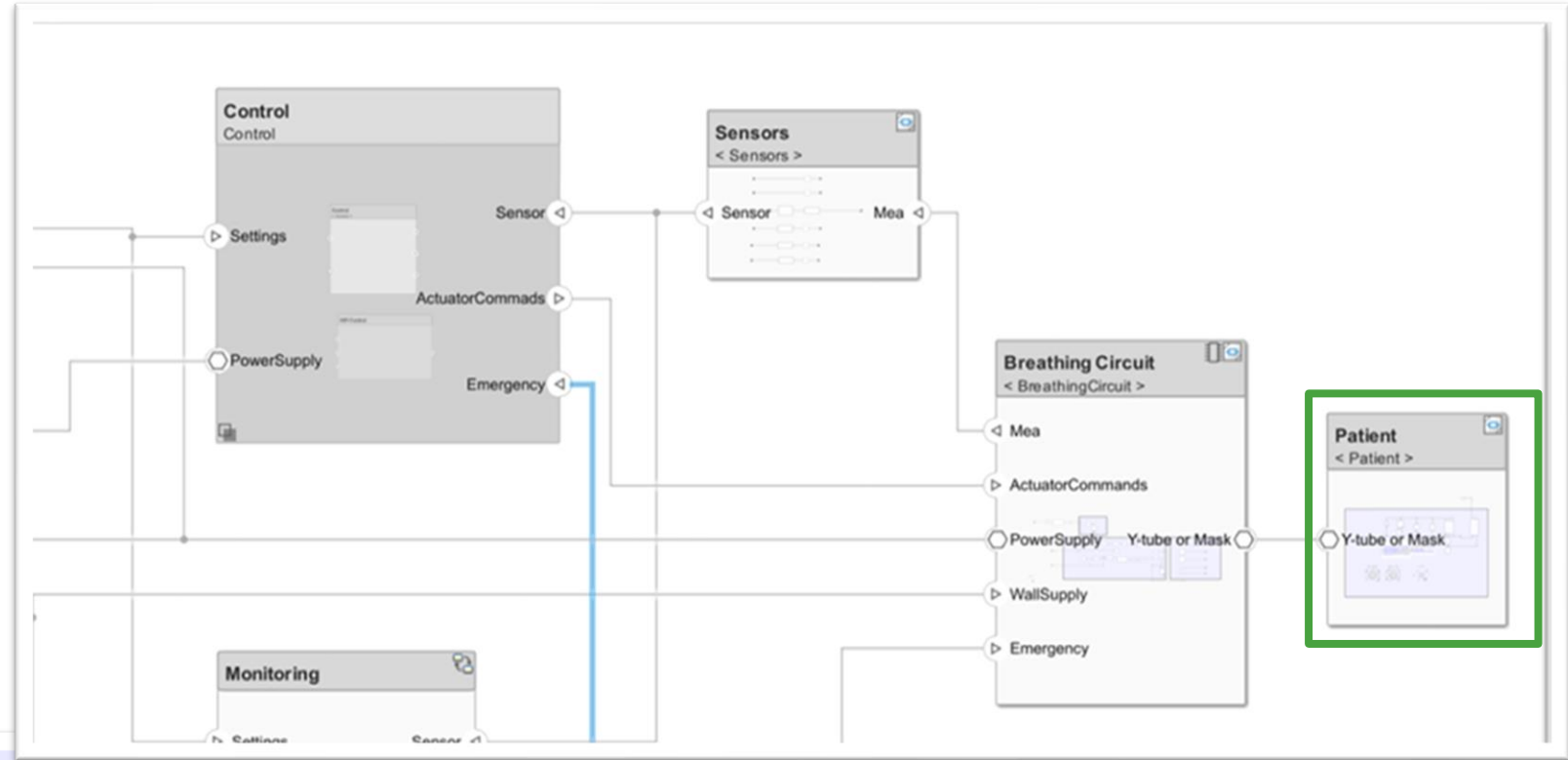
# Collaboration: System Engineer and Control Engineer



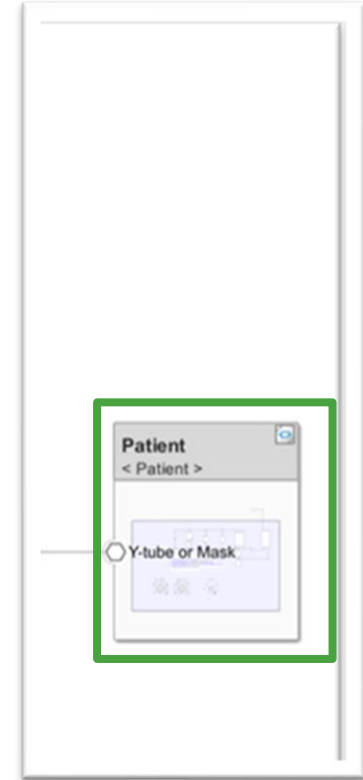
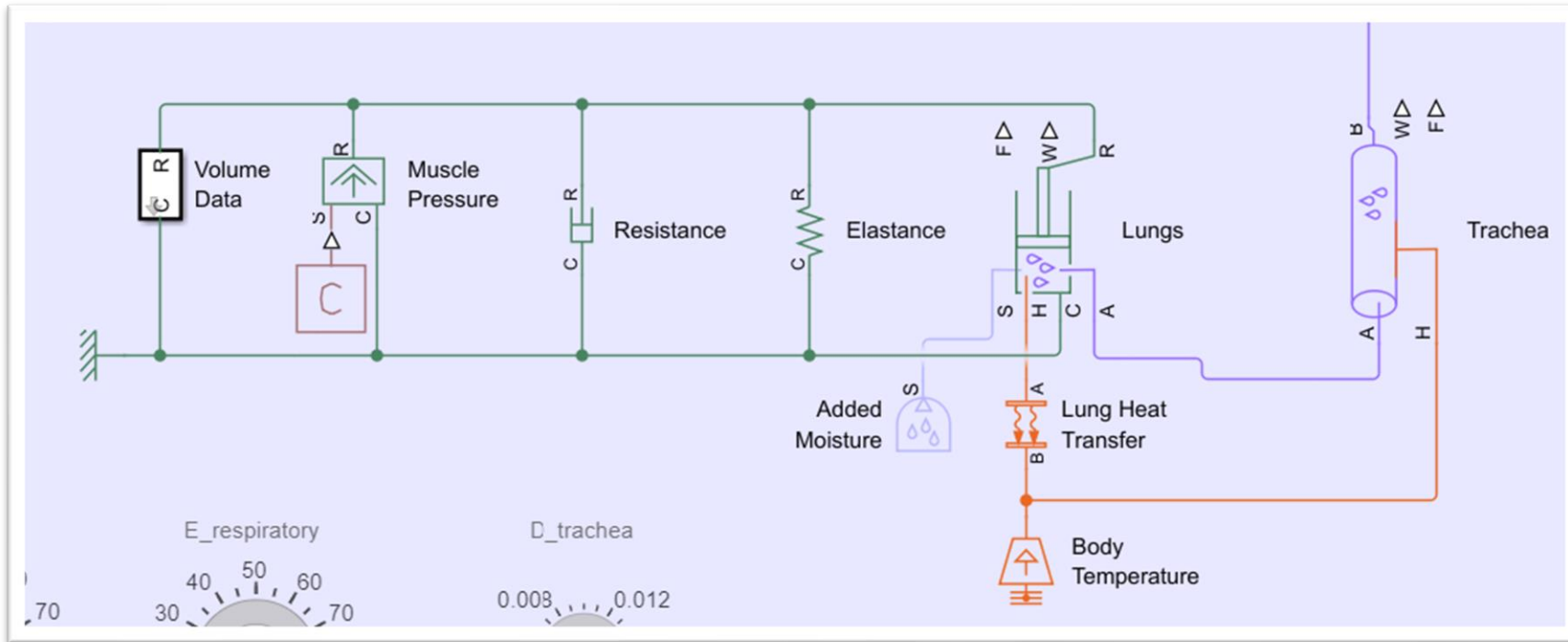
# Collaboration: System Engineer and Control Engineer



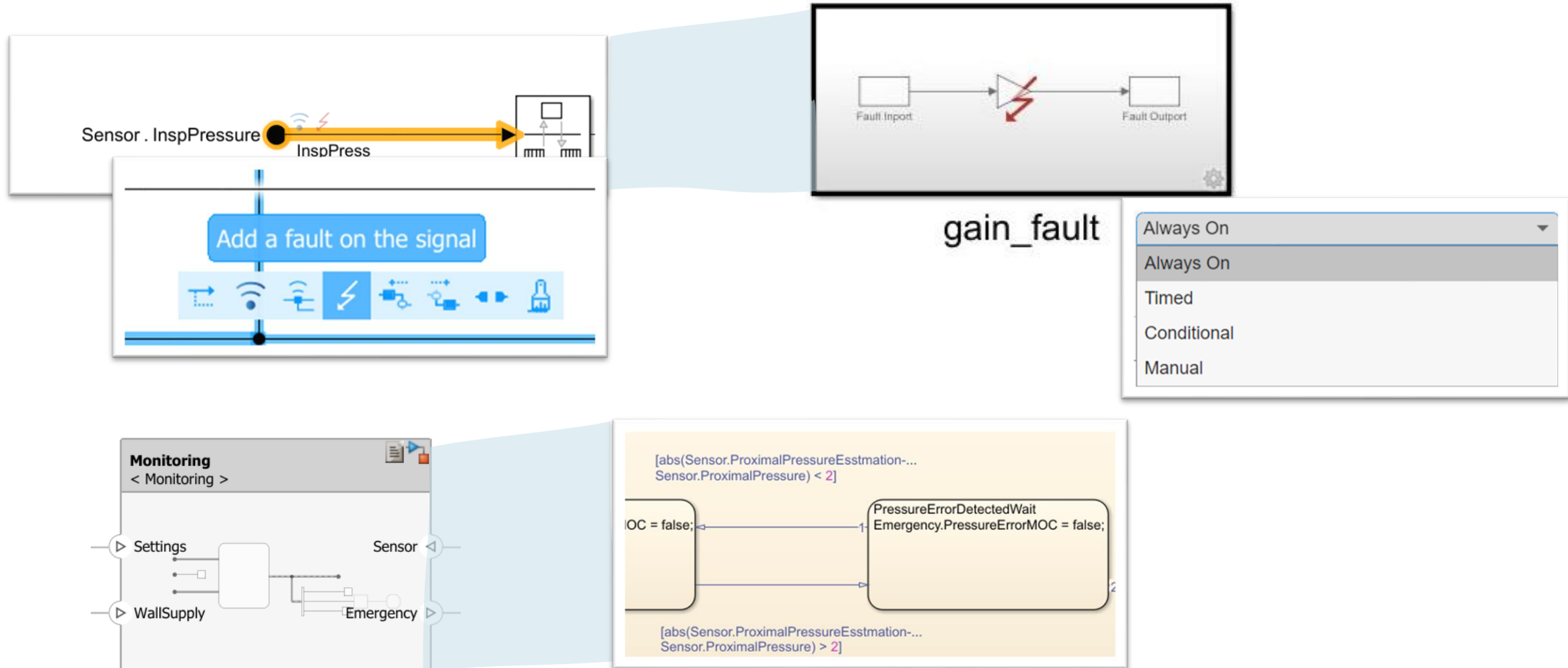
# Collaboration: System Engineer and Control Engineer



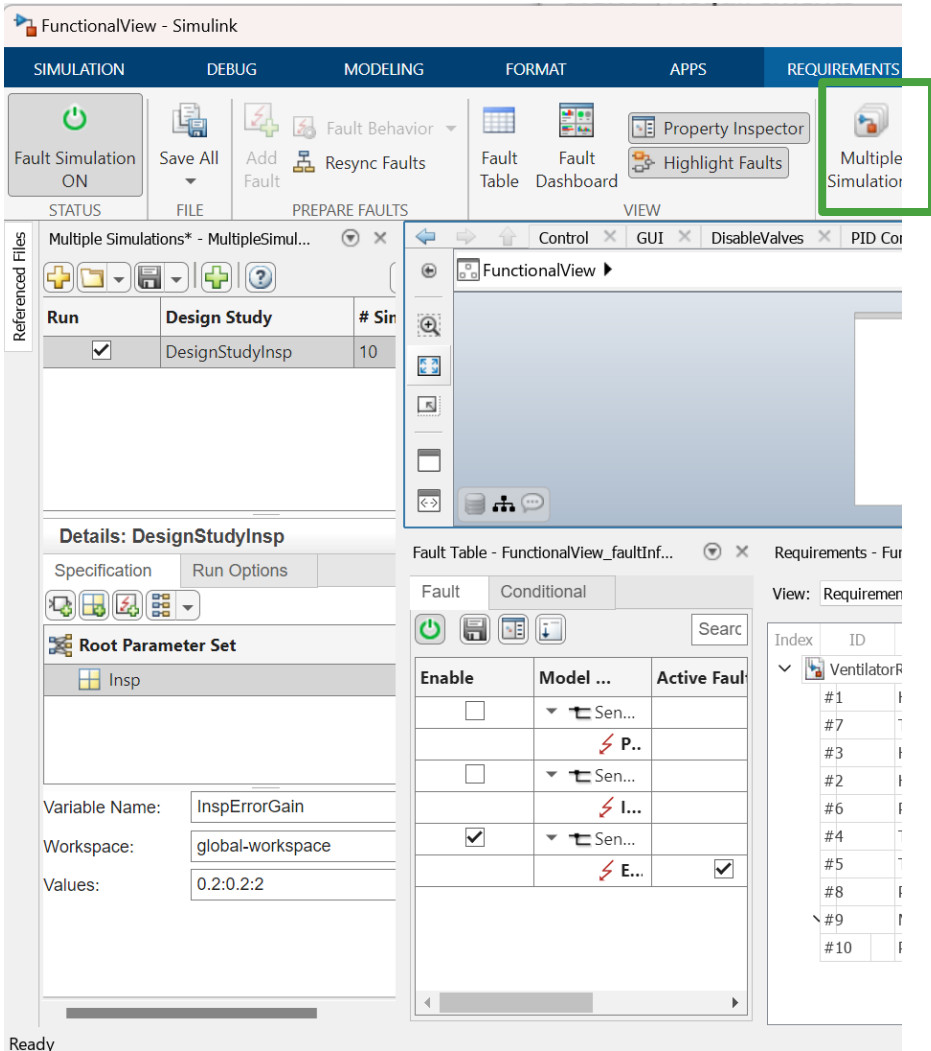
# Collaboration: System Engineer and Control Engineer



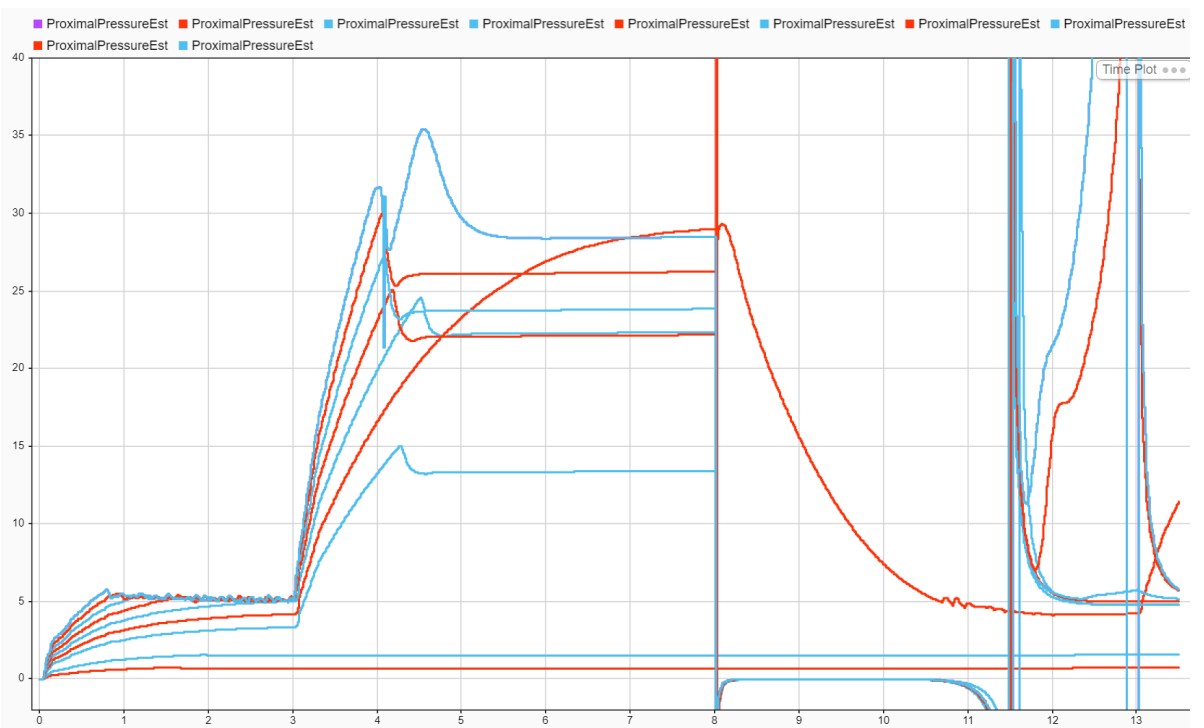
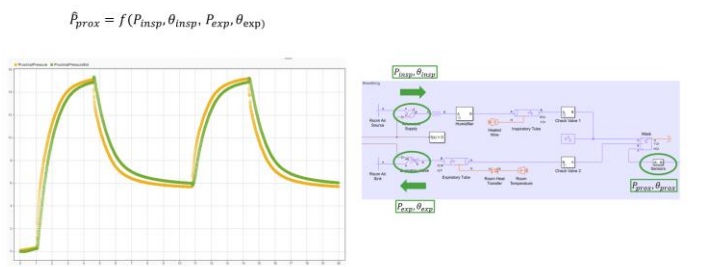
# Injecting Errors and detection method



# Fast, complete, and parallel verification Design Study



Proximal pressure estimator.



# Import FMEA in Excel to Simulink

System	Function	Failure	Severity	Occurance	Detection
Pressure sensor	Proximal Pressure Sensor	PrioximalPressure_fault	10	10	10
Pressure sensor	Insp Pressure Sensor	InspPressure_fault	10	5	10
Pressure sensor	Exp Pressure Sensor	ExpPressure_fault	10	5	10

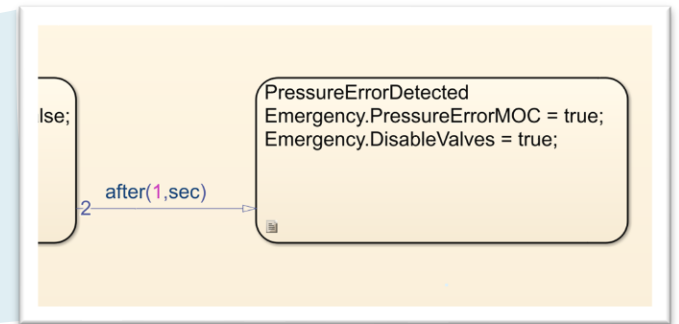
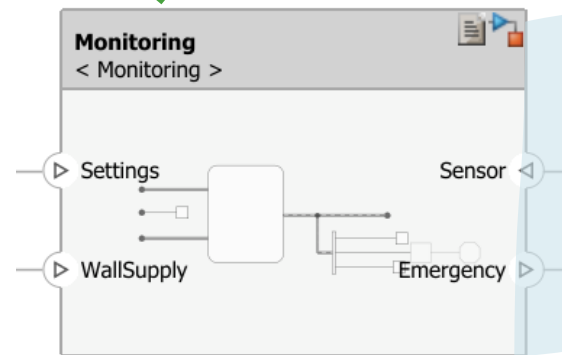
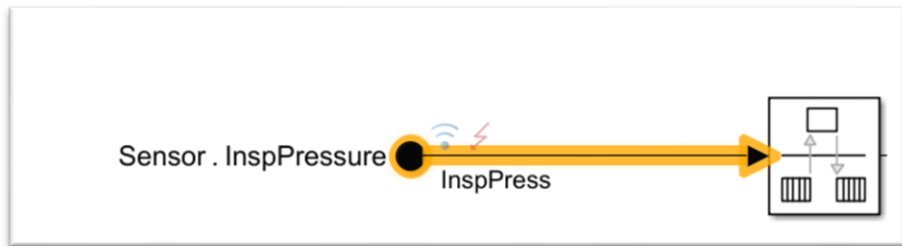
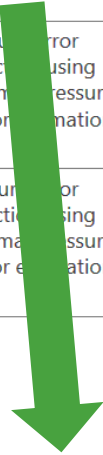
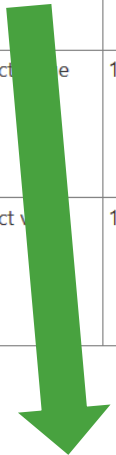
Import

- Empty Spreadsheet
- From Template
  - From Template File
  - MW\_Aerospace\_Templates
    - AFHA
    - SFHA
    - FMEA

n	Failure	Severity	Occurance	Detection	RPN	Detection/MOC	MOC req ref	S	O
ensor	Incorrect value	10	10	10	1000	Pressure Error Detection using Proximal pressure sensor estimation	Link to requirement	10	10
ensor	Incorrect value	10	5	10	500	Pressure Error Detection using Proximal pressure sensor estimation	Link to requirement	10	5
ensor	Incorrect value	10	5	10	500	Pressure Error Detection using Proximal pressure sensor estimation	Link to requirement	10	5

# Automatic MOC verification

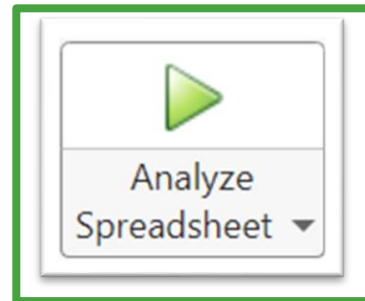
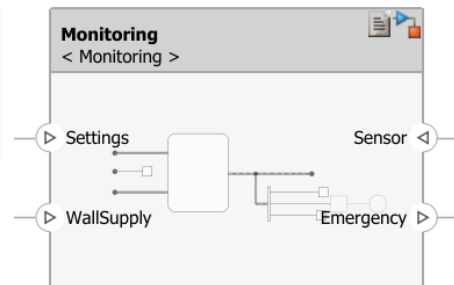
ID	Failure	Severity	Occurance	Detection	RPN	Detection/MOC	MOC req ref	S	O
sensor	Incorrect value	10	10	10	1000	Pressure Error Detection using Proximal pressure sensor estimation	Link to requirement	10	10
sensor	Incorrect value	10	5	10	500	Pressure Error Detection using Proximal pressure sensor estimation	Link to requirement	10	5
sensor	Incorrect value	10	5	10	500	Pressure Error Detection using Proximal pressure sensor estimation	Link to requirement	10	5



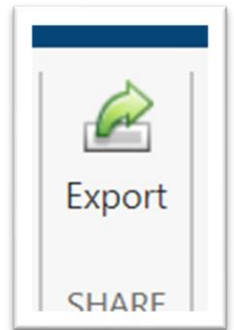


# Automatic MOC verification

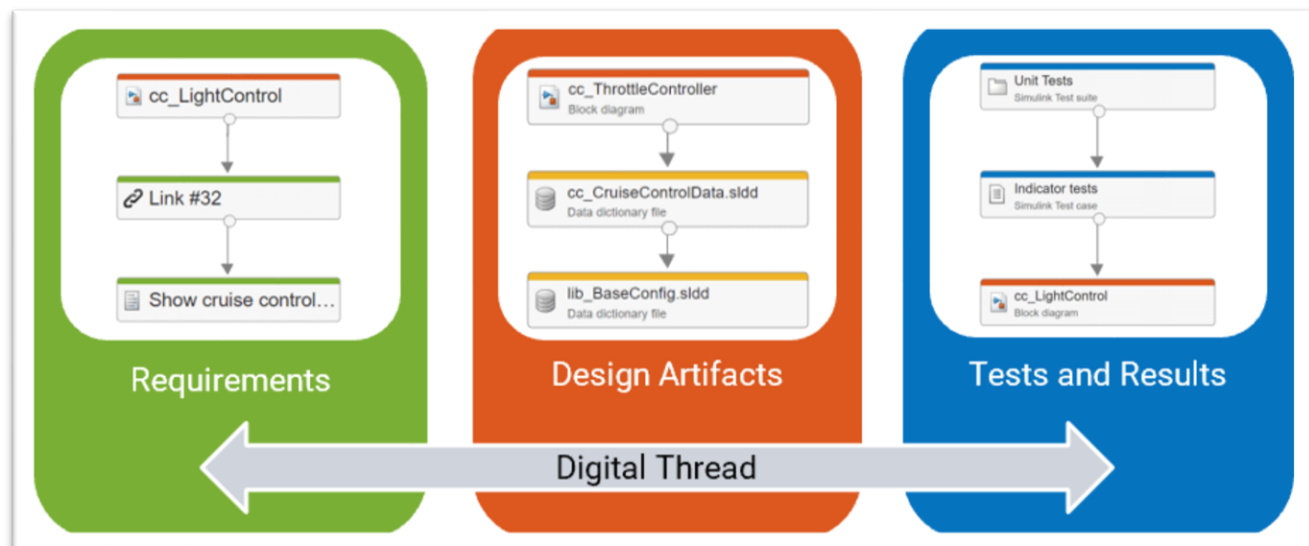
ID	Failure	Severity	Occurance	Detection	RPN	Detection/MOC	MOC req ref	S	O
sensor	Incorrect value	10	10	10	1000	Pressure Error Detection using Proximal pressure sensor estimation	Link to requirement	10	10
sensor	Incorrect value	10	5	10	500	Pressure Error Detection using Proximal pressure sensor estimation	Link to requirement	10	5
sensor	Incorrect value	10	5	10	500	Pressure Error Detection using Proximal pressure sensor estimation	Link to requirement	10	5



Detection/MOC	
Pressure Error Detection using Proximal pressure sensor estimation	✓
Pressure Error Detection using Proximal pressure sensor estimation	✓
Pressure Error Detection using Proximal pressure sensor estimation	✓



# Digital Thread



	Failure	Local Effect	System Effect	S	Po	Detection	RPN	Detection/MOC	MOC req ref
re	Incorrect value <a href="#">Link</a>	Incorrect pressure control. Higher true pressure if control pressure is falsly lower.	Possible barotrauma.	8	8	10	640	Pressure Error Detection using Proximal pressure sensor estimation <a href="#">✓</a> <a href="#">Link</a>	When pressure error is detected the disable valves shall be set to true, stopping ventilation and activate high level alarm. <a href="#">Link</a>
	Incorrect value <a href="#">Link</a>	Incorrect pressure control. Higher true pressure if control pressure is falsly lower.	Possible barotrauma.	8	5	10	400	Pressure Error Detection using Proximal pressure sensor estimation <a href="#">✓</a> <a href="#">Link</a>	When pressure error is detected the disable valves shall be set to true, stopping ventilation and activate high level alarm. <a href="#">Link</a>
	Incorrect value <a href="#">Link</a>	Incorrect pressure control. Higher true pressure if control pressure is falsly lower.	Possible barotrauma.	8	5	10	400	Pressure Error Detection using Proximal pressure sensor estimation <a href="#">✓</a> <a href="#">Link</a>	When pressure error is detected the disable valves shall be set to true, stopping ventilation and activate high level alarm. <a href="#">Link</a>

# Digital Thread

Requirements - Monitoring

View: Requirements

Index	ID	Summary
▼		VentilatorRequirements
#1		HighPressureAlarm
#7		TimeAtHighPressure
#3		HighPressureAlarmInformation
#2		HighPressureEmergencyEvacuation
#6		PeakPressureDuringEvacuation
#4		The maximum pressure during emergency evacuation
#5		The HighPressureAlarm deactivation
#8		Proximal Estimation Error
#9		MOC requirements from FMEA
#10		Pressure Error Detection

Po	Detection	RPN	Detection/MOC	MOC req ref
8	10	640	Pressure Error Detection using Proximal pressure sensor estimation ✓ <a href="#">link</a>	When pressure error is detected the disable valves shall be set to true, stopping ventilation and activate high level alarm.  <a href="#">link</a>
5	10	400	Pressure Error Detection using Proximal pressure sensor estimation ✓ <a href="#">link</a>	When pressure error is detected the disable valves shall be set to true, stopping ventilation and activate high level alarm.  <a href="#">link</a>
5	10	400	Pressure Error Detection using Proximal pressure sensor estimation ✓ <a href="#">link</a>	When pressure error is detected the disable valves shall be set to true, stopping ventilation and activate high level alarm.  <a href="#">link</a>

# Collaboration: System Engineer and Test Engineer

## Reuse of Faults

The screenshot displays the Test Manager application interface. The top menu bar includes options for FILE, EDIT, RUN, RESULTS, ENVIRONMENT, and RESOURCES. The main workspace is divided into two panes: 'Test Browser' and 'Results and Artifacts'.

**Test Browser:** A search filter is set to 'test'. The test hierarchy is expanded to show 'Simscape-Medical-Ventilator' > 'High Pressure Error' > 'High Pressure Error - Normal Condition'.

**Results and Artifacts:** The selected test case is displayed with the following details:

- High Pressure Error - Normal Condition**
- [Simscape-Medical-Ventilator](#) » [High Pressure Error](#) » [High Pressure Error - Normal Condition](#)
- Baseline Test
- Create Test Case from External File
- ▶ TAGS
- ▶ DESCRIPTION
- ▶ REQUIREMENTS\*
- ▼ SYSTEM UNDER TEST\*

# Collaboration: System Engineer and Test Engineer

## Reuse of Faults

Test Manager

TESTS

FILE EDIT RUN

Test Browser Results and Artifacts

Filter tests by name or tags, e.g. tags: test

- Simscape-Medical-Ventilator
  - High Pressure Error
    - High Pressure Error - Normal Condition
    - High Pressure Error - Fault in pressure sensor
    - High Pressure Error - Control Signal Error 150%
  - Proximal Sensor Estimation
    - ProximalEstimator
      - ProximalEstimator - Fault in InspPressure Sensor 80%
      - ProximalEstimator - Fault in ProximalPressureSensor Error 70%

Sen

AL ASSESSMENTS\*

FAULT NAME

TRIGGER

MODEL ELEMENT

ExpPressure\_fault

InspPressure\_fault

PrioximalPressure\_fault

Always On

Always On

Timed: 4

OK Cancel

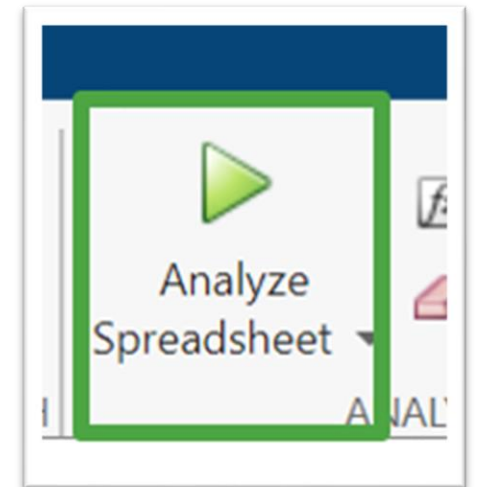
If the list of faults is incomplete, click to refresh.



## Another great reason to automate your FMEA

The FMEA should be updated whenever:

- A new cycle begins (new product/process)
- Changes are made to the operating conditions
- A change is made in the design
- New regulations are instituted
- Customer feedback indicates a problem



# Questions?





# MATLAB EXPO

 FRANCE



© 2024 The MathWorks, Inc. MATLAB and Simulink are registered trademarks of The MathWorks, Inc. See [mathworks.com/trademarks](https://www.mathworks.com/trademarks) for a list of additional trademarks. Other product or brand names may be trademarks or registered trademarks of their respective holders.

