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

MathWorks

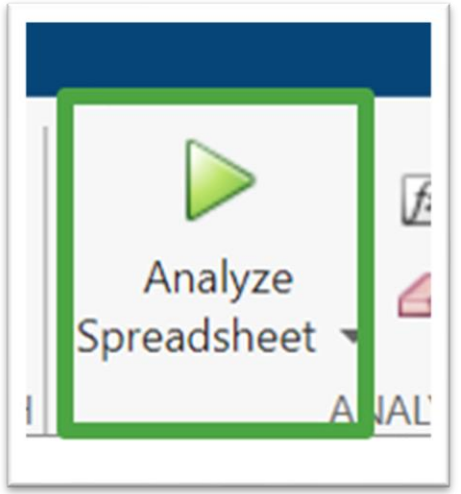
Agenda

Background

or Extended ×

	Failure	Local Effect	System Effect	S	Po
ure	Incorrect value	Incorrect pressure control.	Possible barotrauma.	8	8
		pressure if control pressure is falsly lower.			

Problem Definition



Solution

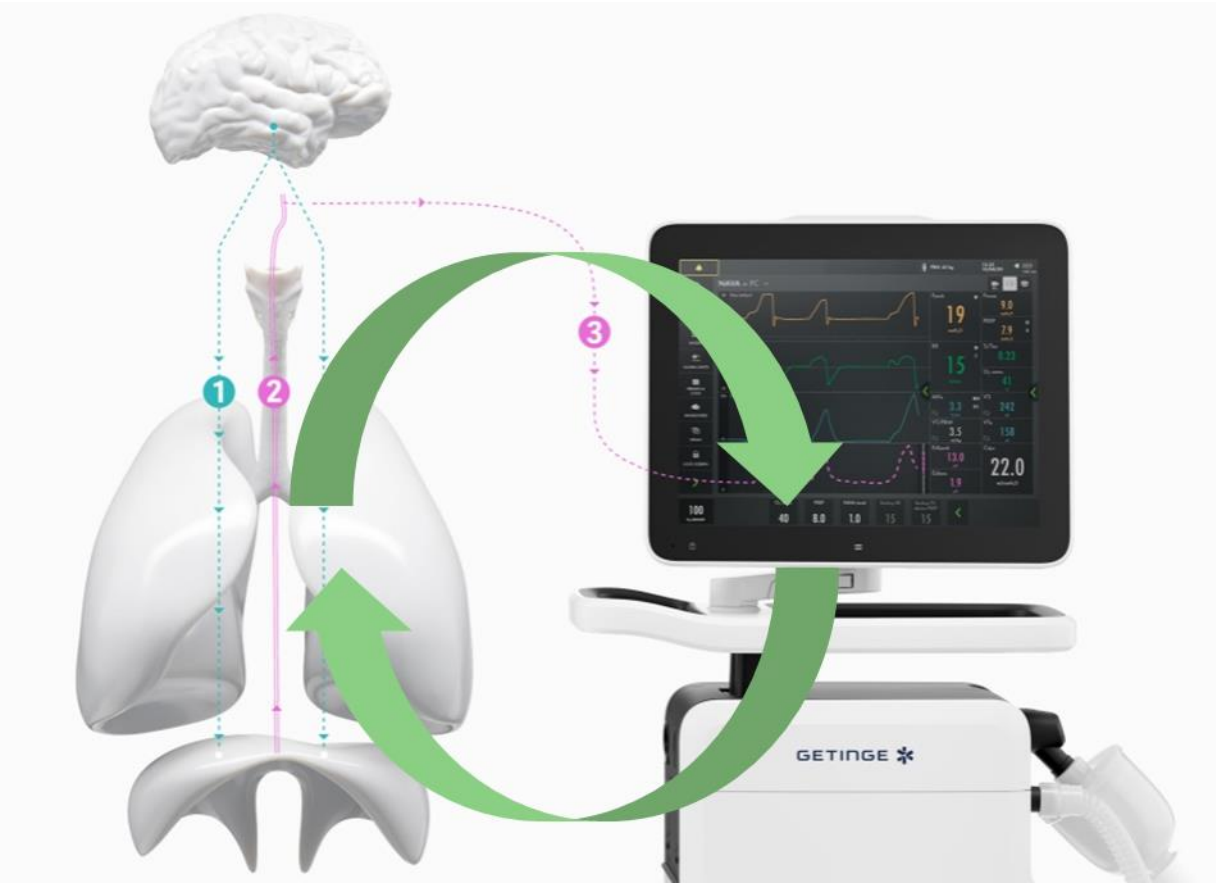
GETINGE

Anesthesia Machine

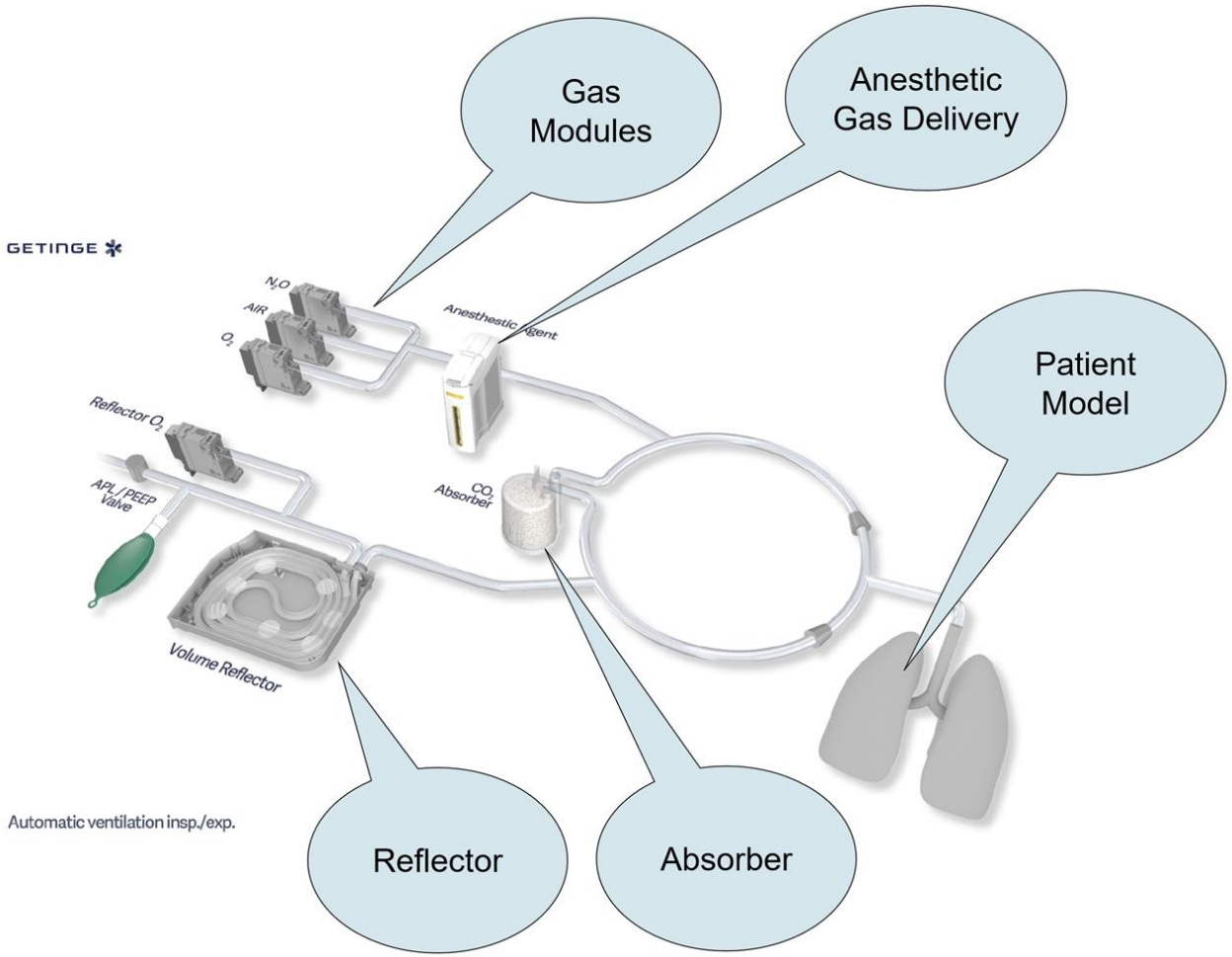
- Founded in 1904
- 12000 employees
- 40 countries
- First ventilator with valves and control loops.
- The world's first Implantable Pacemaker

Mechanical Ventilator

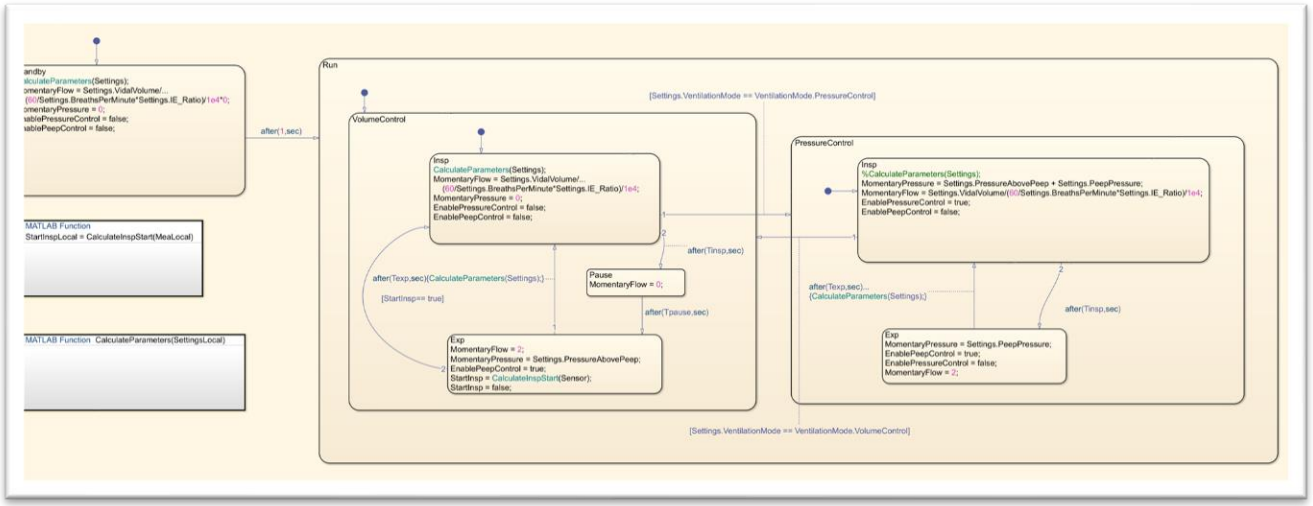
Getinge

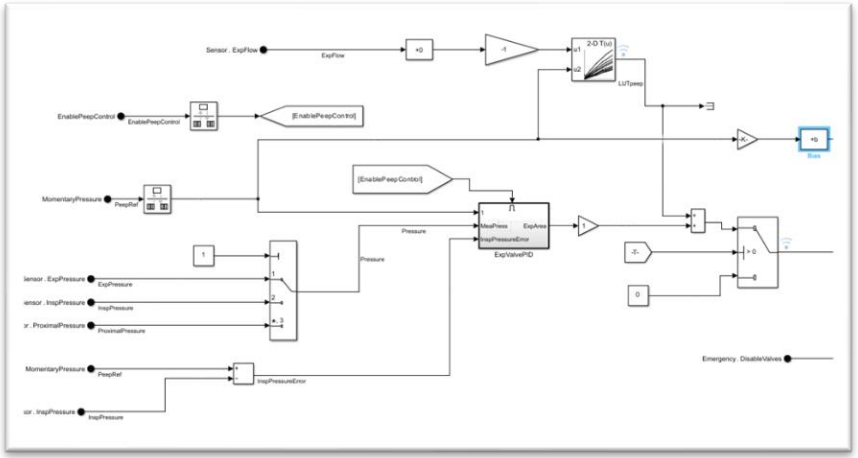


Getinge


Gas Modules
Anesthetic Gas Delivery
Patient Model
Reflector
Absorber
GETINGE
Automatic ventilation insp./exp.

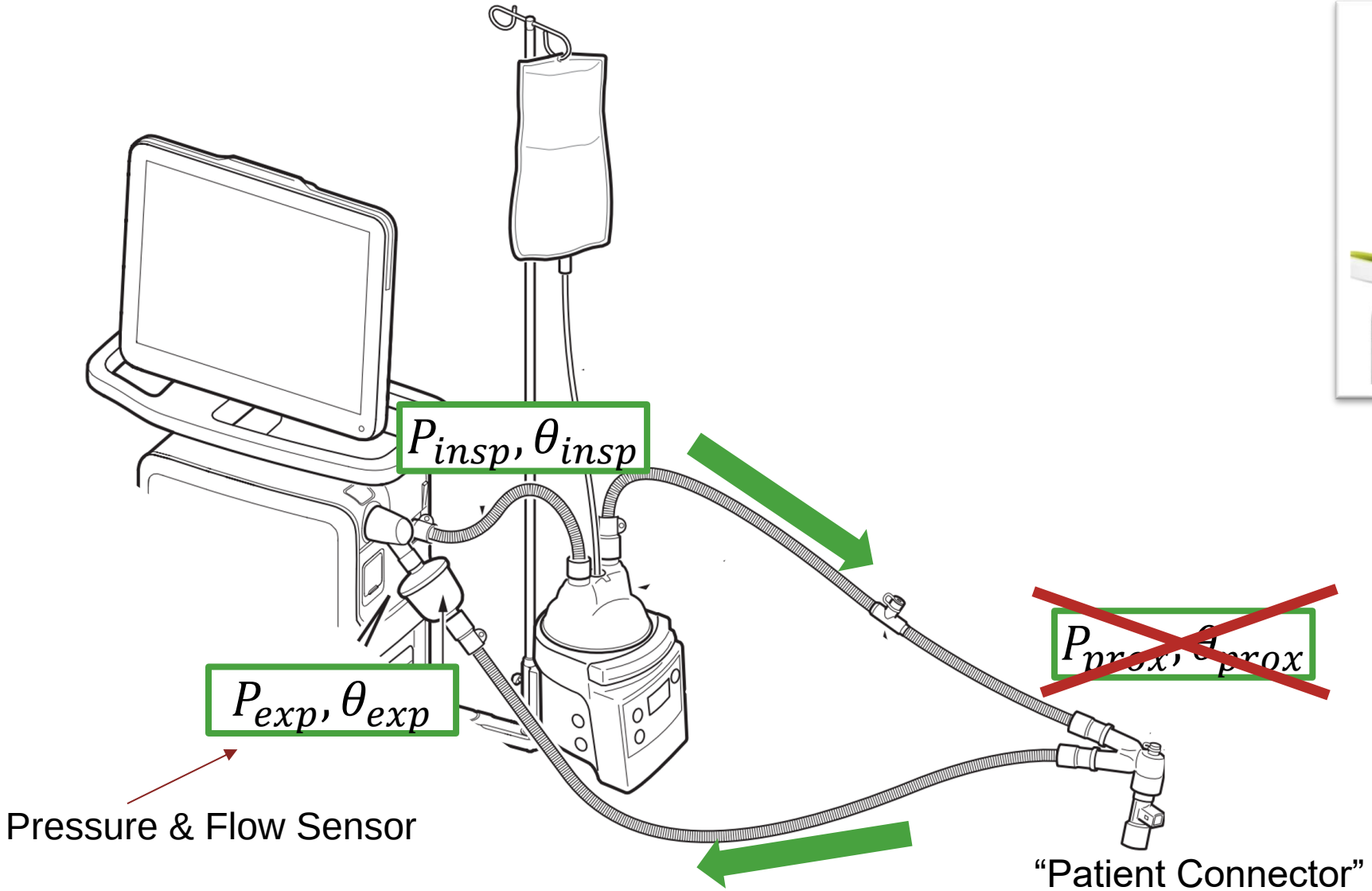
Getinge


Run
[Settings.VentilationMode == VentilationMode.PressureControl]
VolumeControl
PressureControl
Insp
Pause
MomentaryFlow = 0;
Exp
after(1,sec)
after(Tinsp,sec)
after(Tpause,sec)
[StartInsp== true]
[Settings.VentilationMode == VentilationMode.VolumeControl]


Sensor . ExpFlow
EnablePeepControl
[EnablePeepControl]
MomentaryPressure
Pressure
Emergency. DisableValves


GETINGE

The mechanical Ventilator – What could go wrong?



Risk Management vs FMEA

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

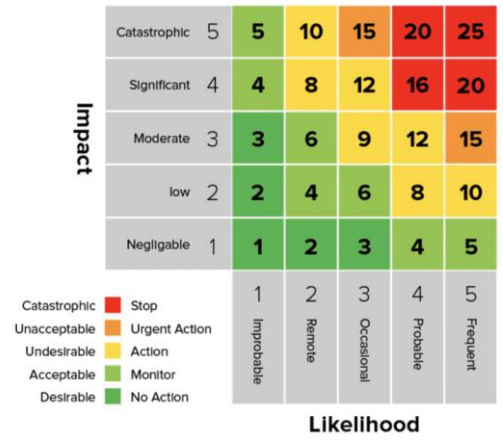
Risk Management vs FMEA

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

FMEA (IEC 60812)

Automated FMEA for a ventilator Extended

	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	0



FMECA

Typical FMEA work

Automated FMEA for a ventilator Extended

	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

	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

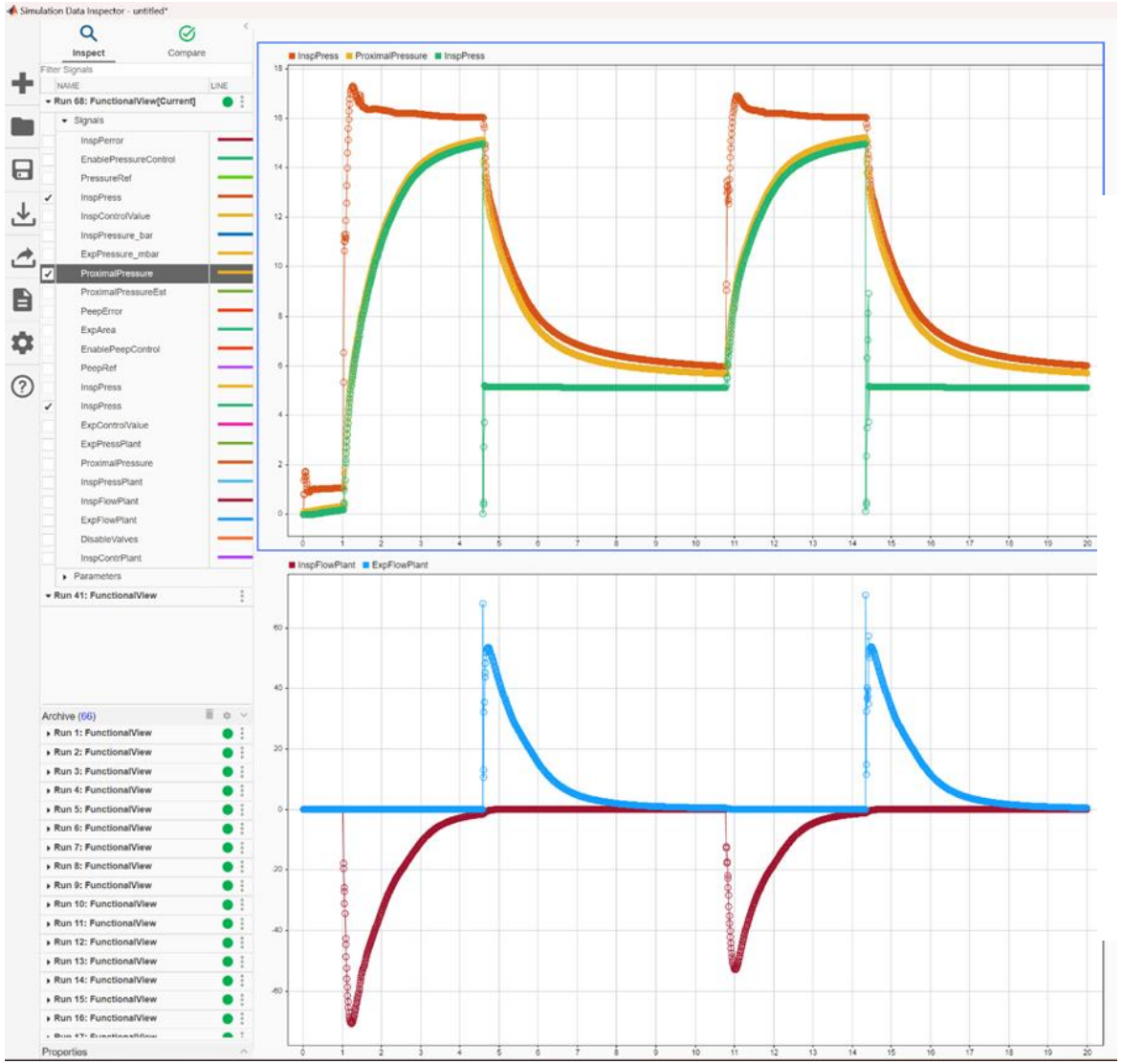
Automated FMEA for a ventilator Extended

	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

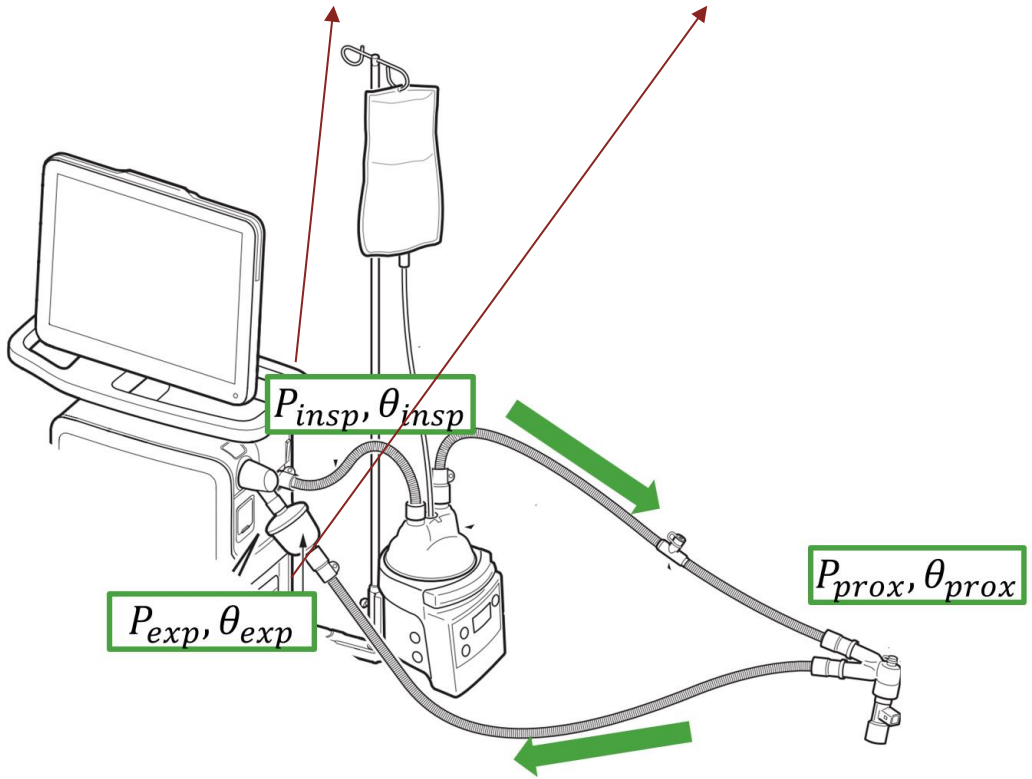
RPN = S*Po*Detection = 8 * 8 * 10 = 640

Risk Priority Number

The mechanical Ventilator – redundancy.



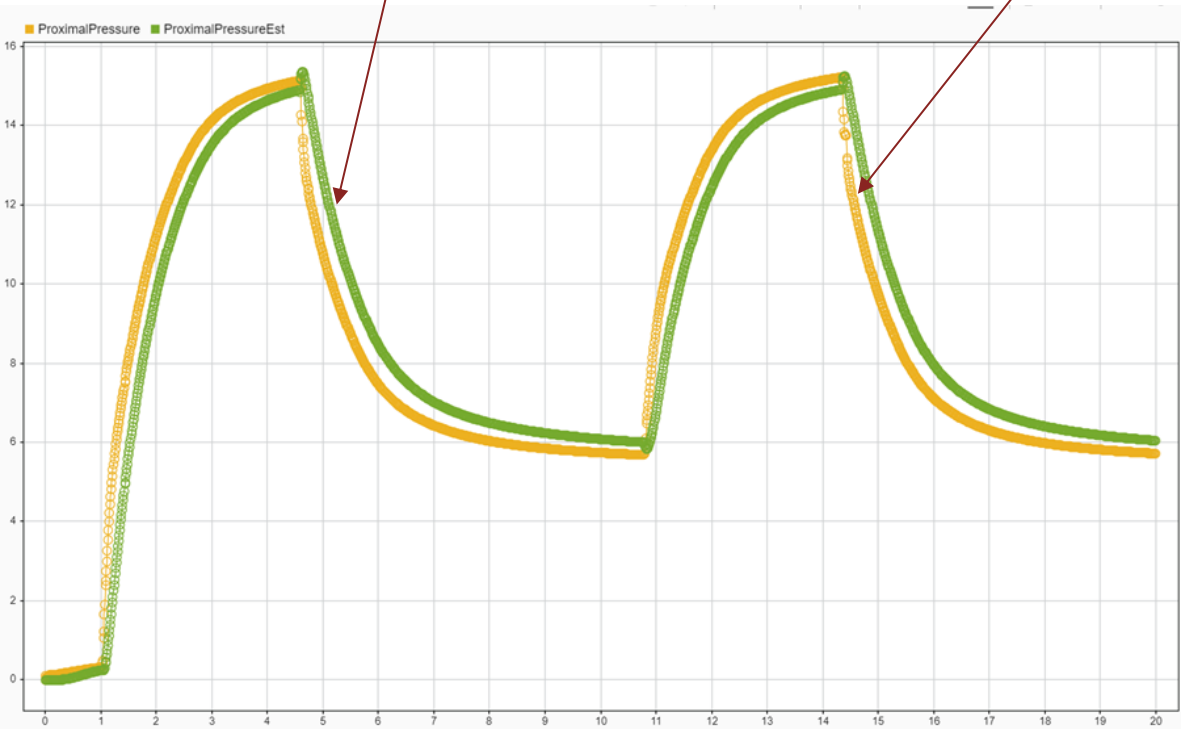
$$\hat{P}_{prox} = f(P_{insp}, \theta_{insp}, P_{exp}, \theta_{\exp})$$

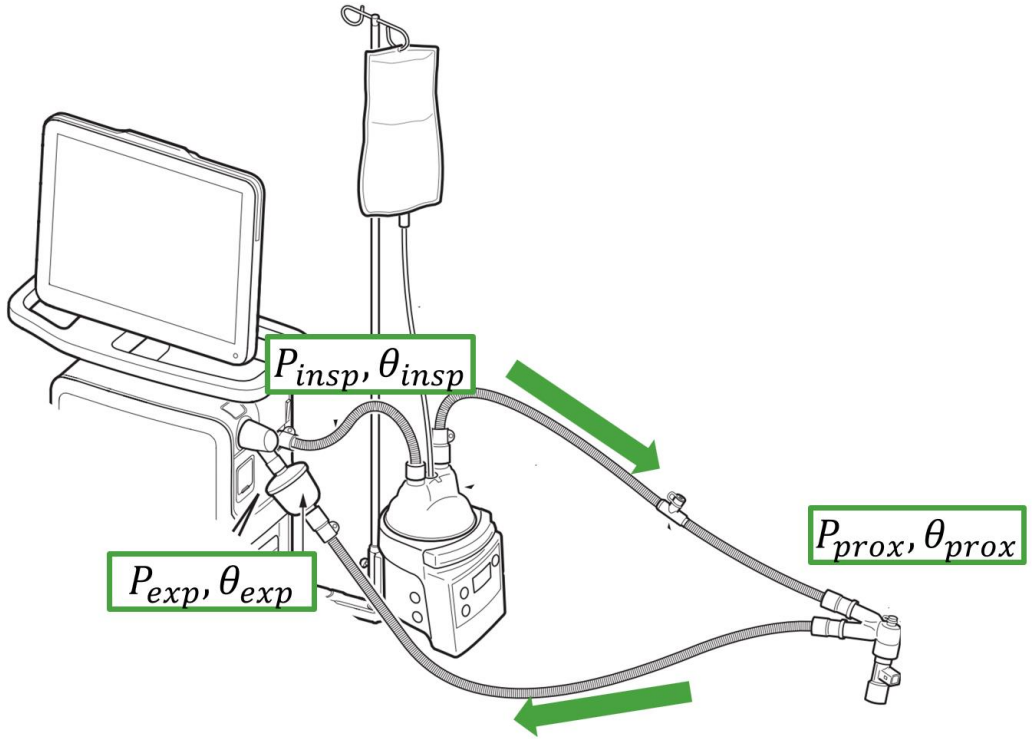


The mechanical Ventilator – redundancy.

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

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

RPN = S*Po*Detection = 8 * 8 * 1 = 64

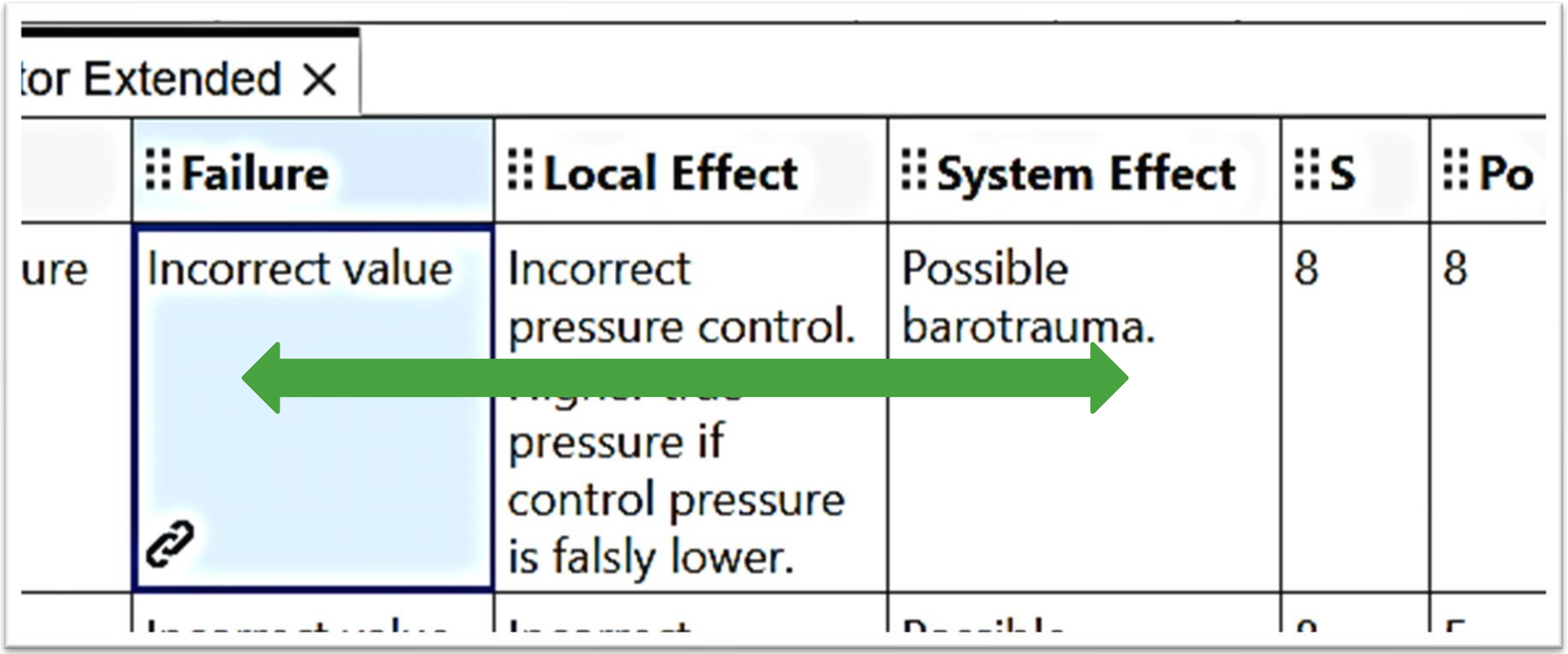
Typical FMEA work

Where are the problems with a manual workflow?

Automated FMEA for a ventilator Extended

	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



Complicated cause and effect reasoning

Typical FMEA work

tor Extended ×

	Failure	Local Effect	System Effect	S	Po	Detection	RPN	Detection/MOC	MOC req ref
ure	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 activ

Complicated cause and effect reasoning

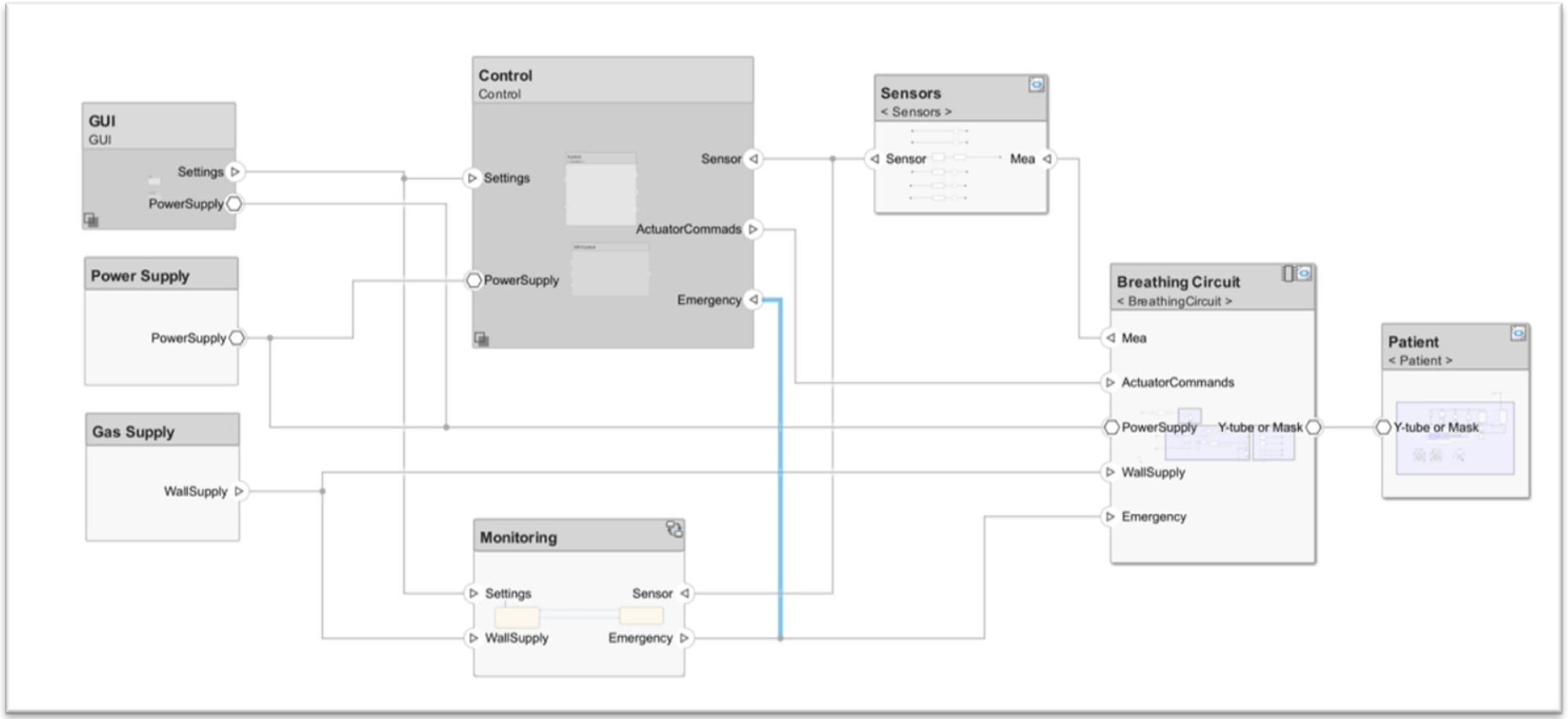
Is the MOC really solving the problem?

Manual labour

Error prone

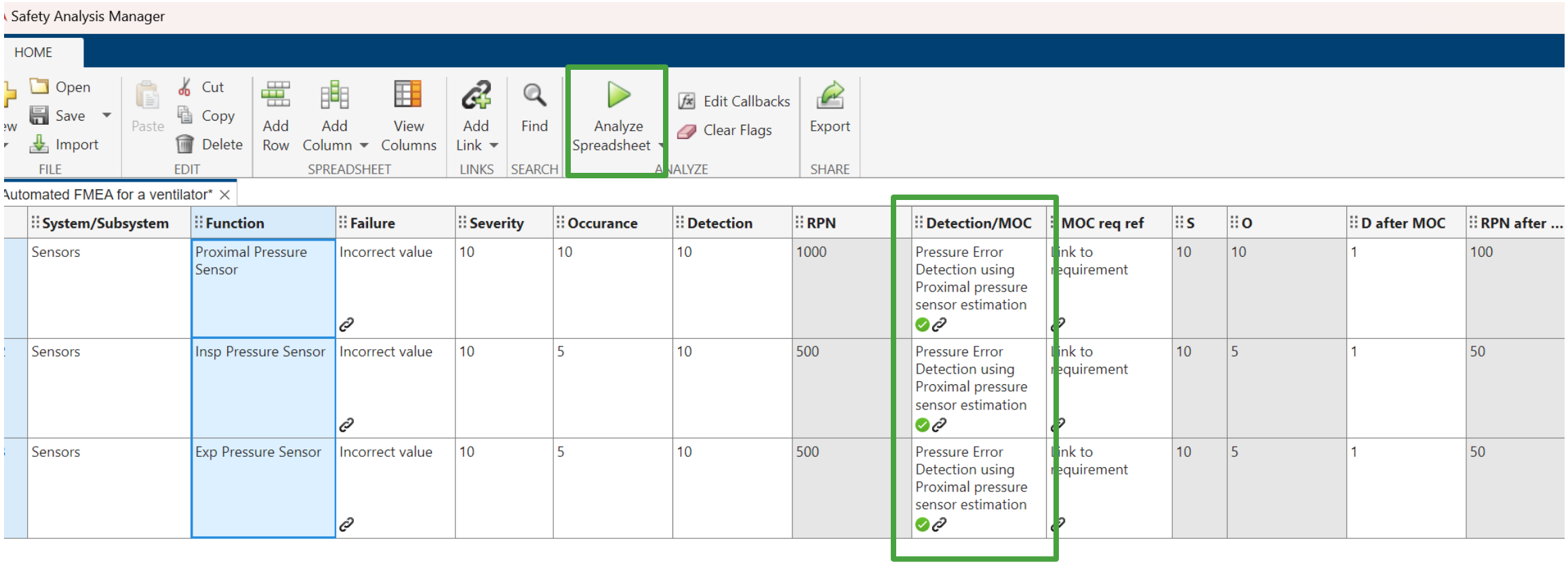
What if you could…

Manage the system level design and….



What if you could…

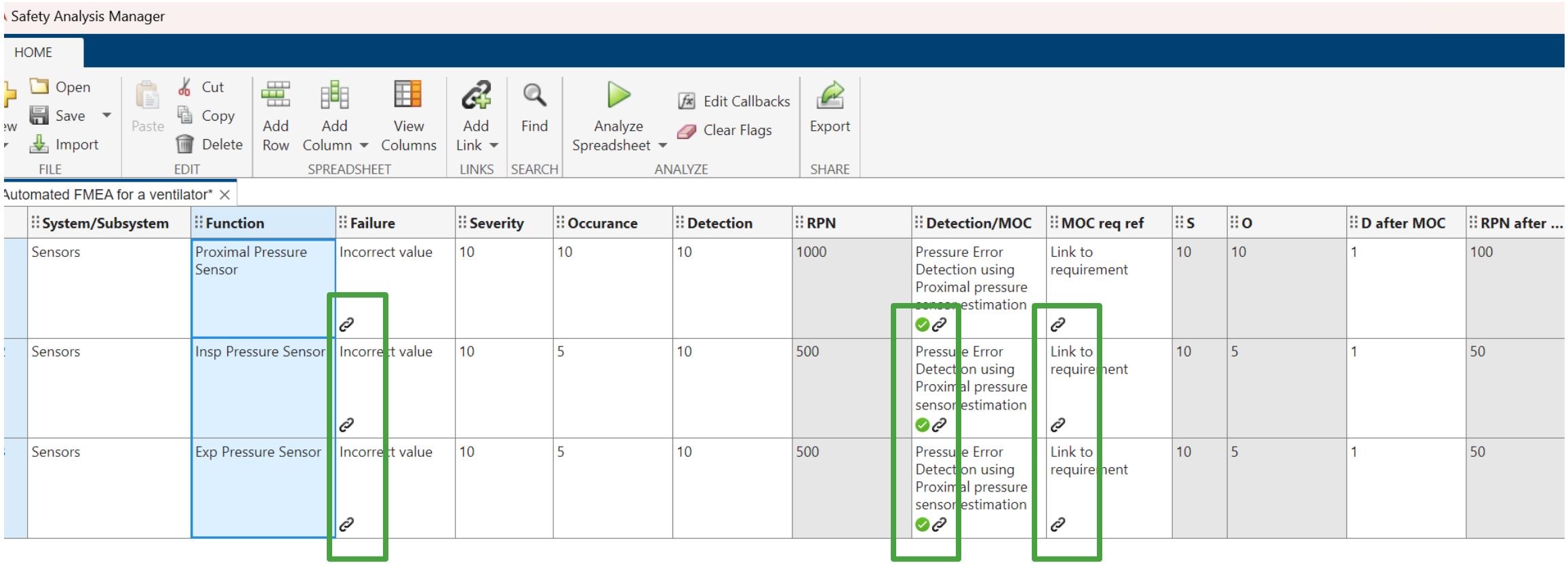
Automate the FMEA MOC verification…



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…

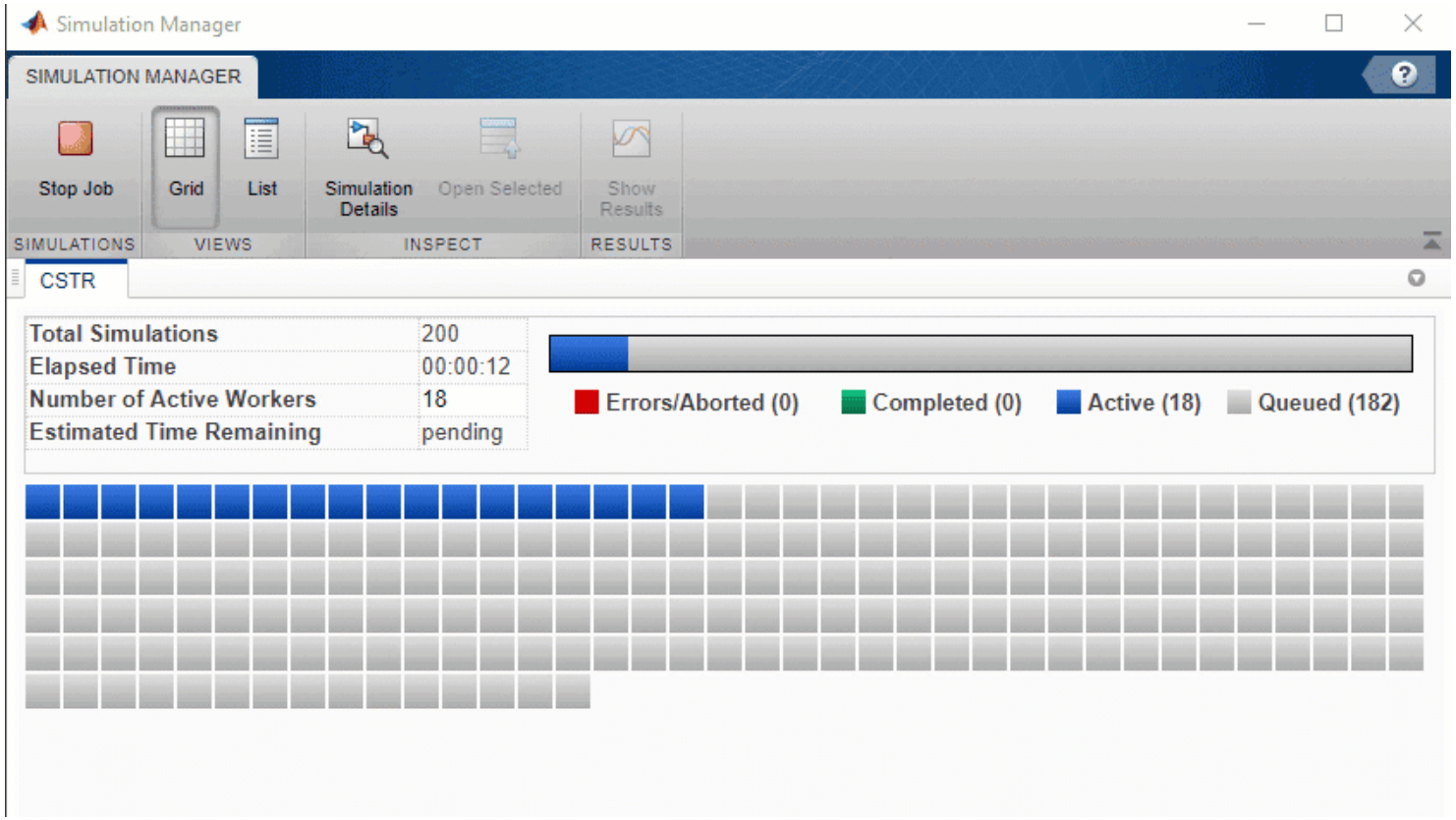
Safeguard the digital thread throughout the project…



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…

Speed up extensive MOC validation …



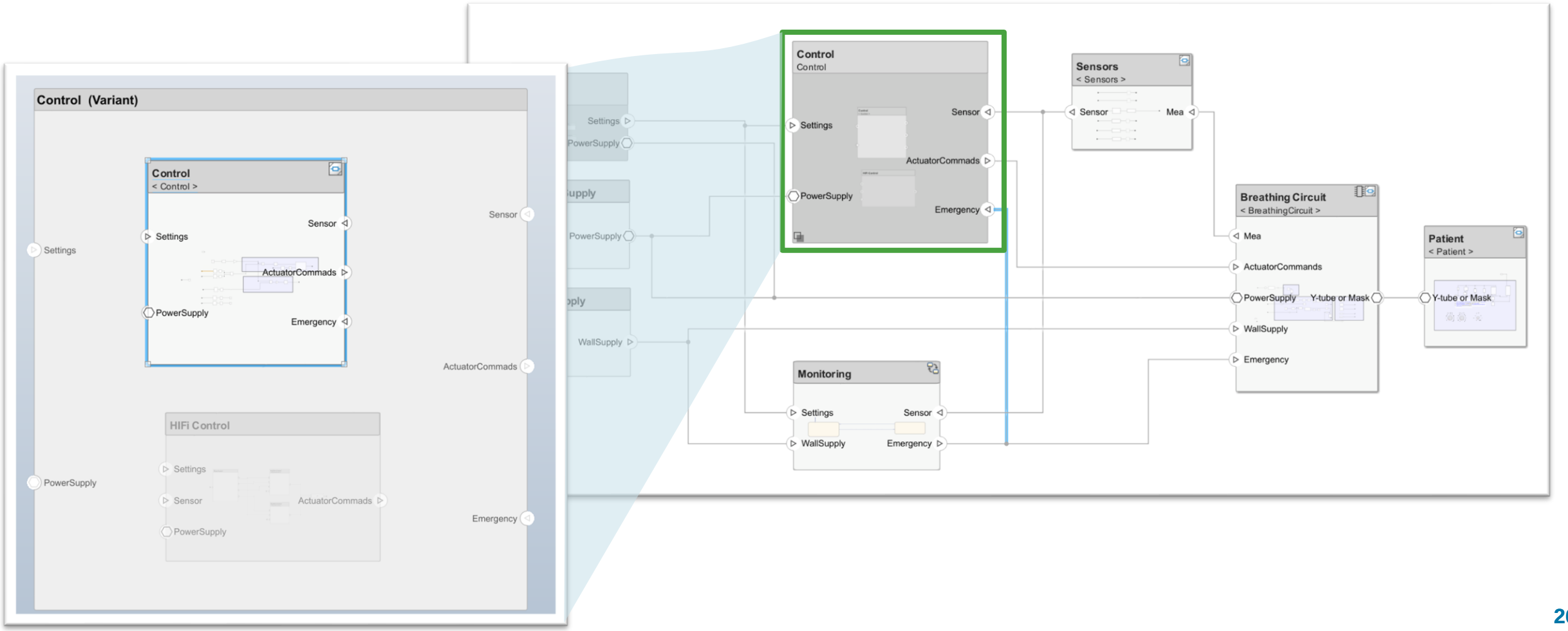
Permutations on

- Pressure above Peep
- Peep
- Tidal Volume
- I_E ratio
- Breath Rate
- Patient Resistance
- Patient Compliance

10 000 to 100 000 permutations

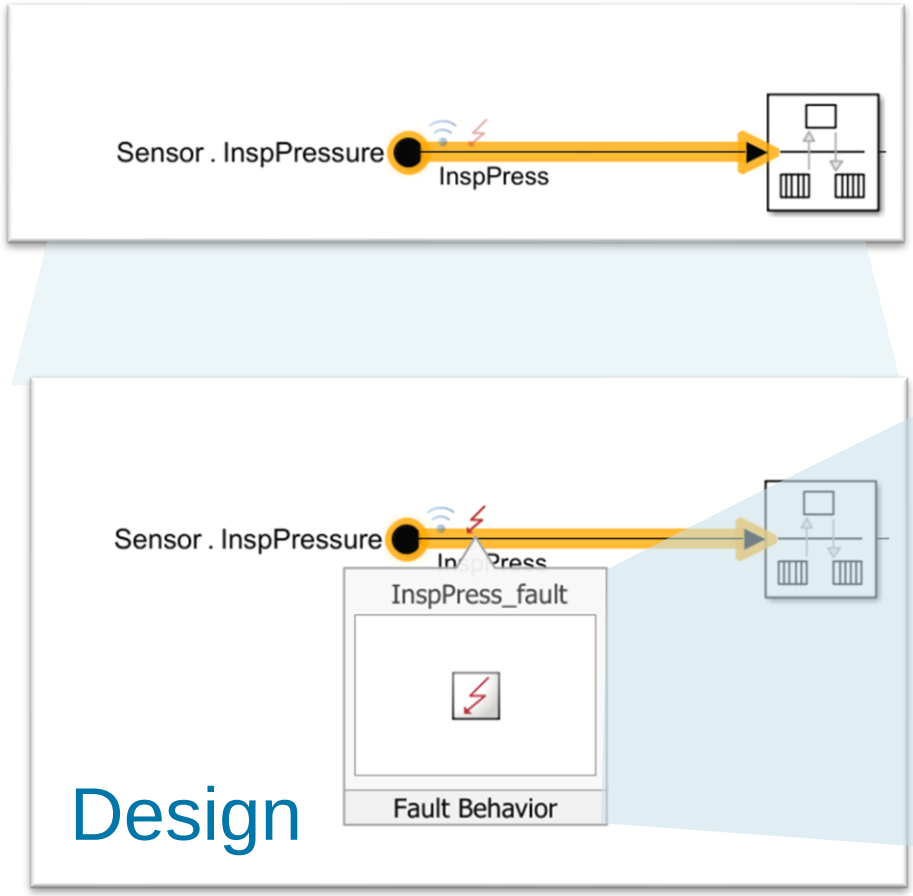
What if you could…

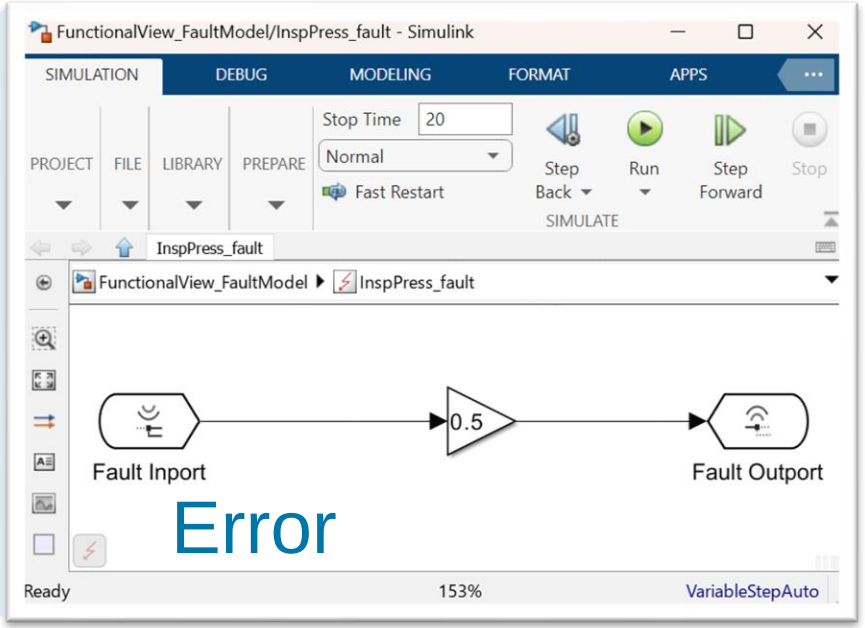
Ensure effective collaboration across your team.…



What if you could…

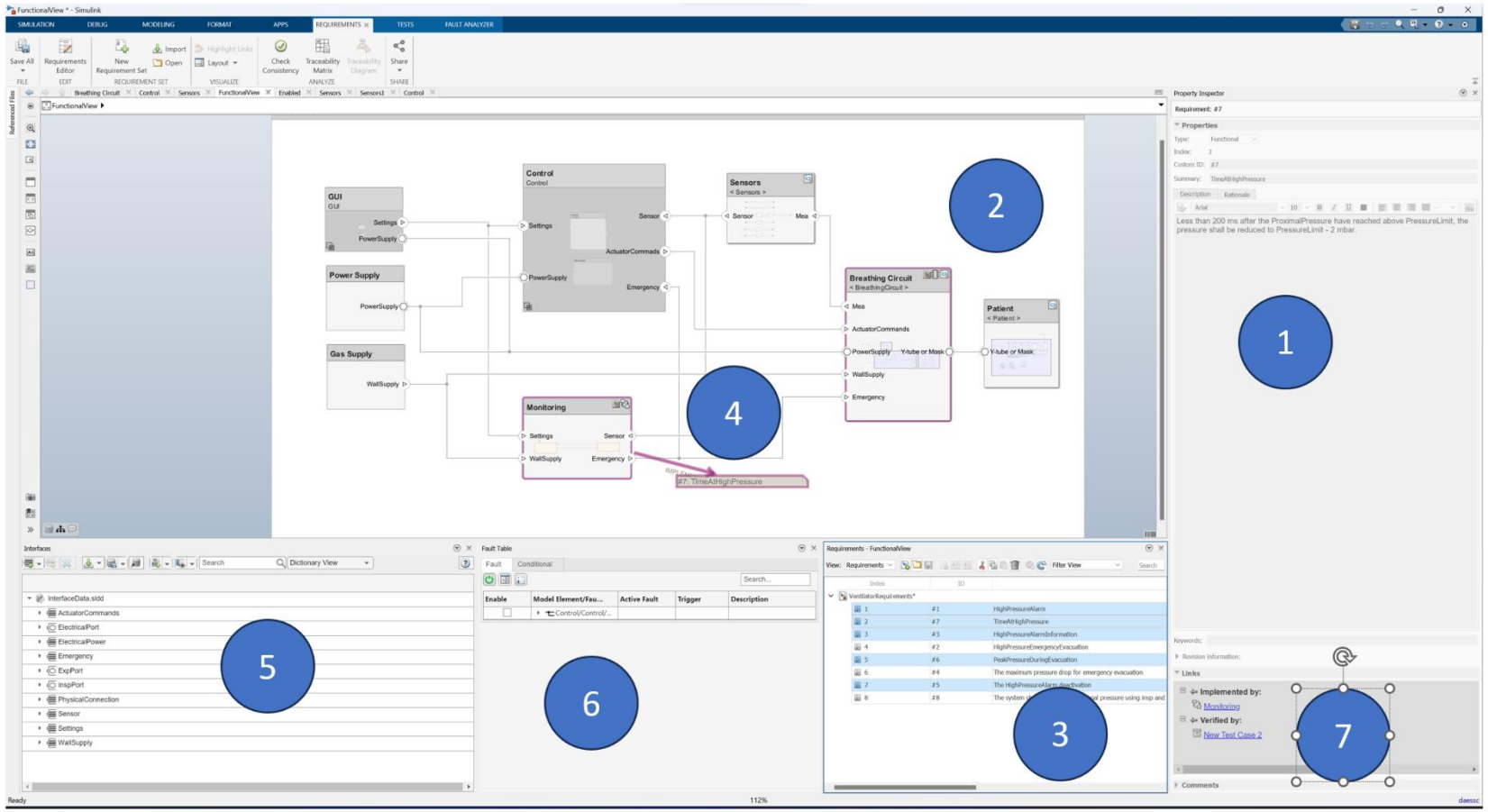
Separate your design from your faults…



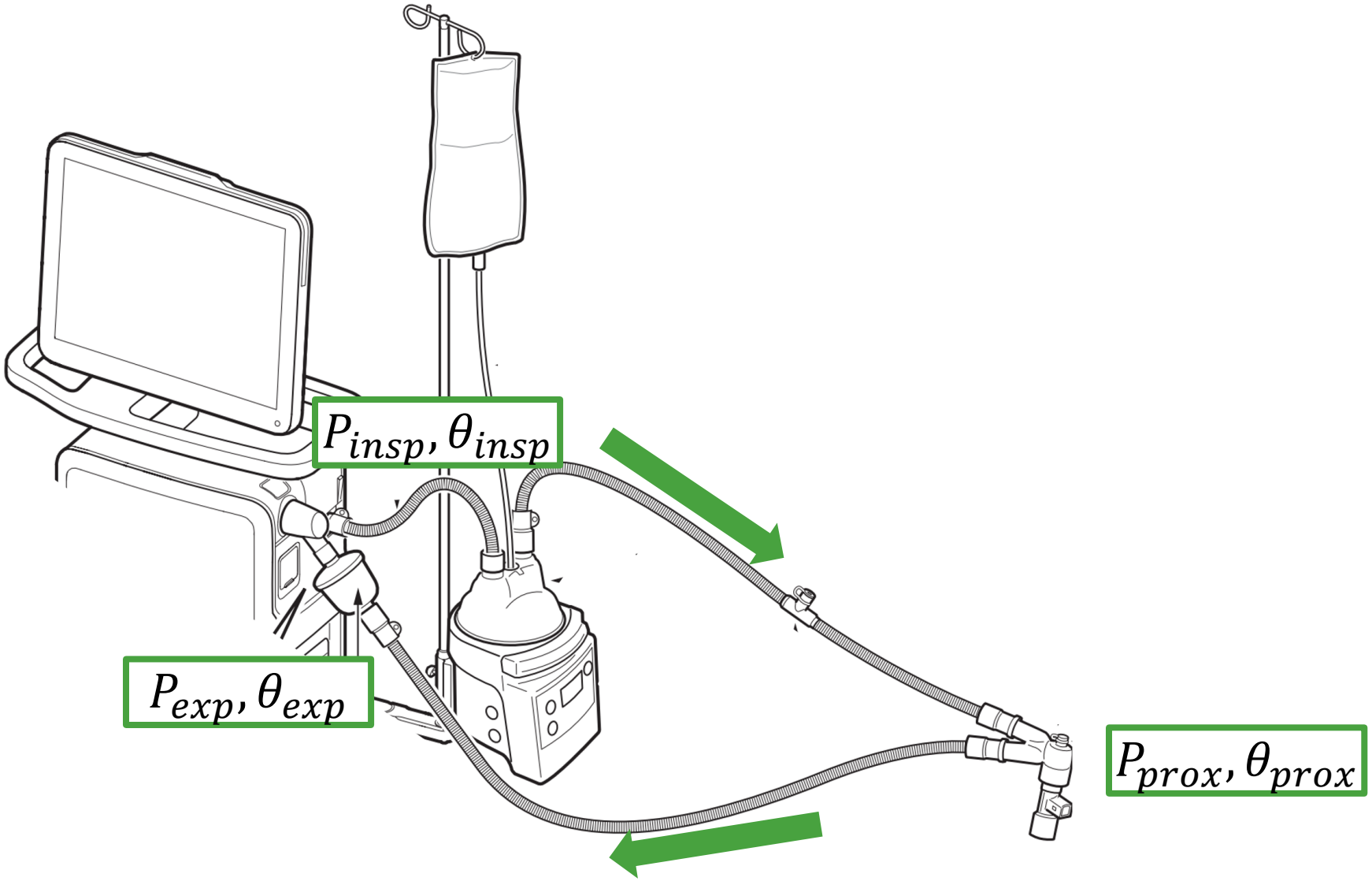


What if you could…

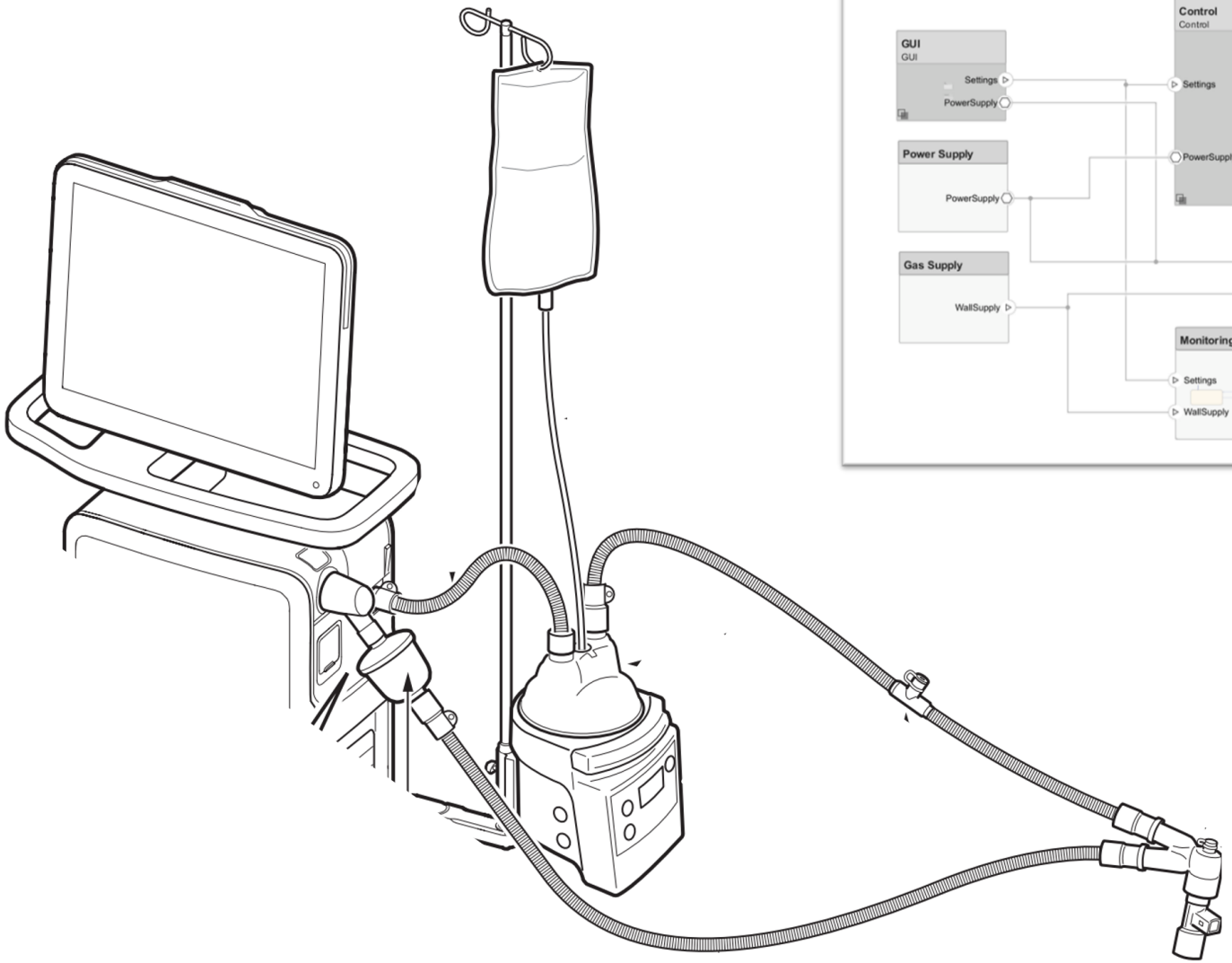
Have everything in reach using a model centric workflow…

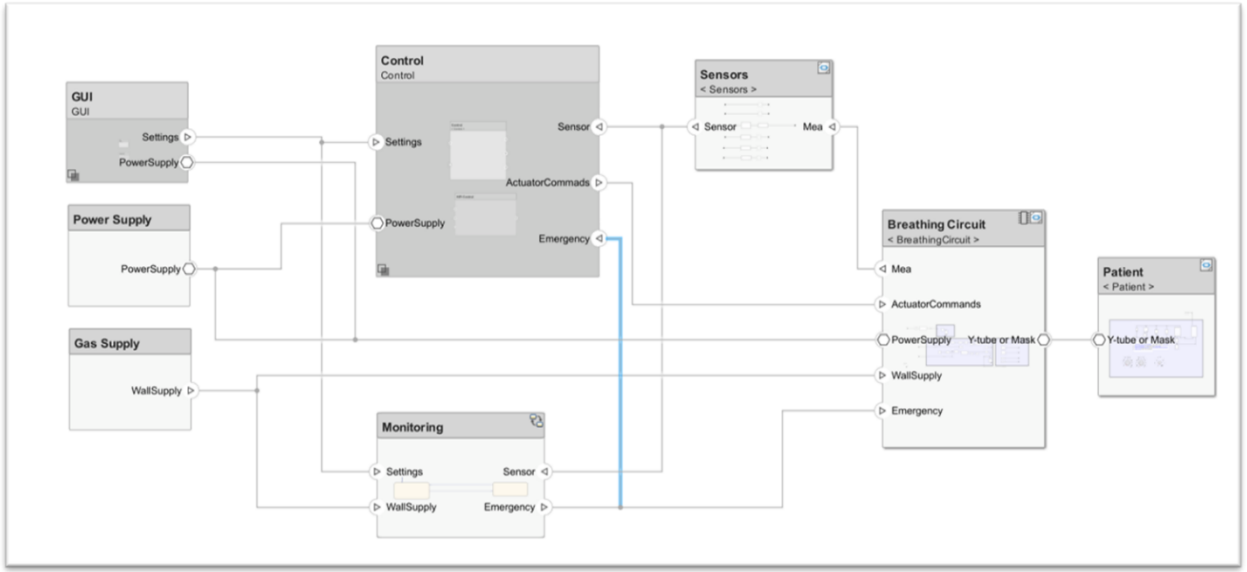


The Mechanical Ventilator



Adding models to your System Engineering

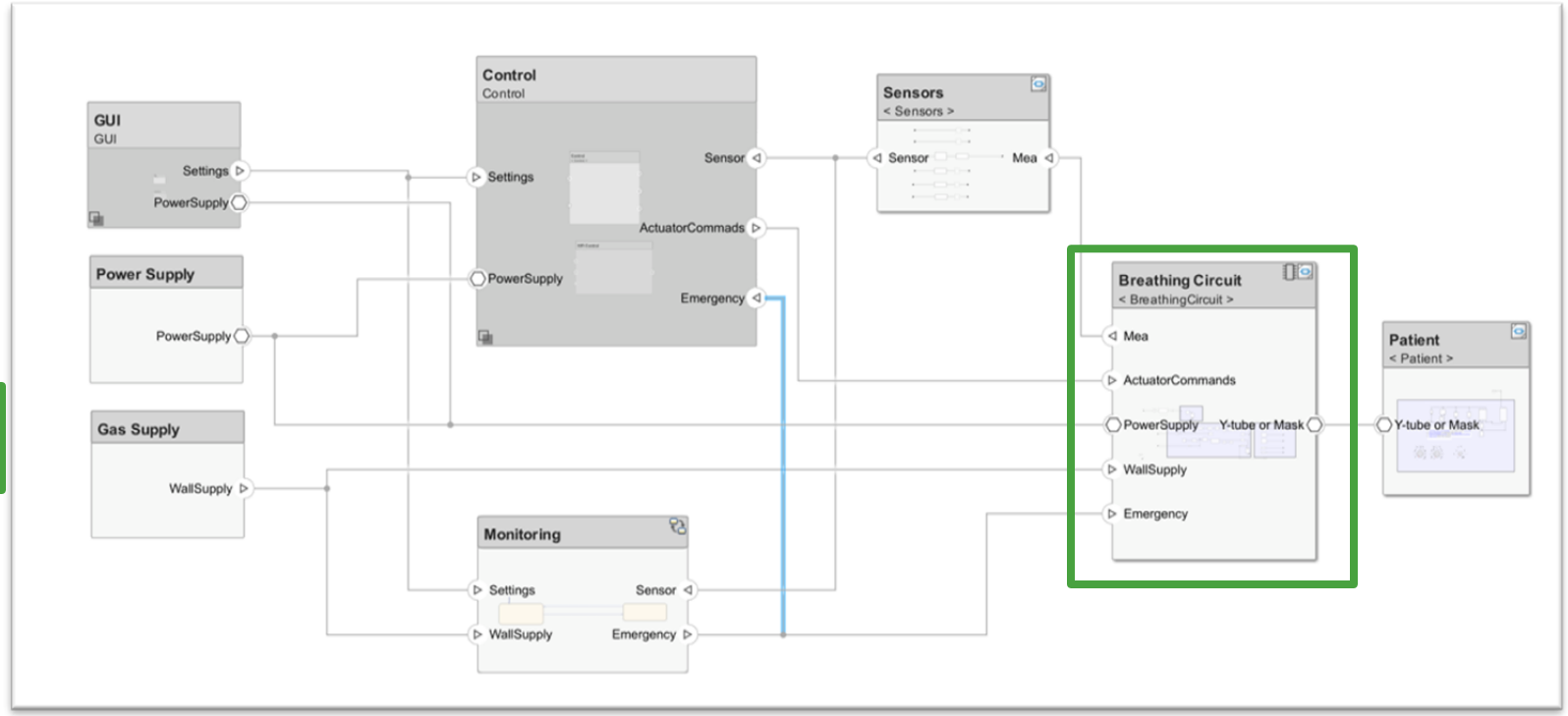




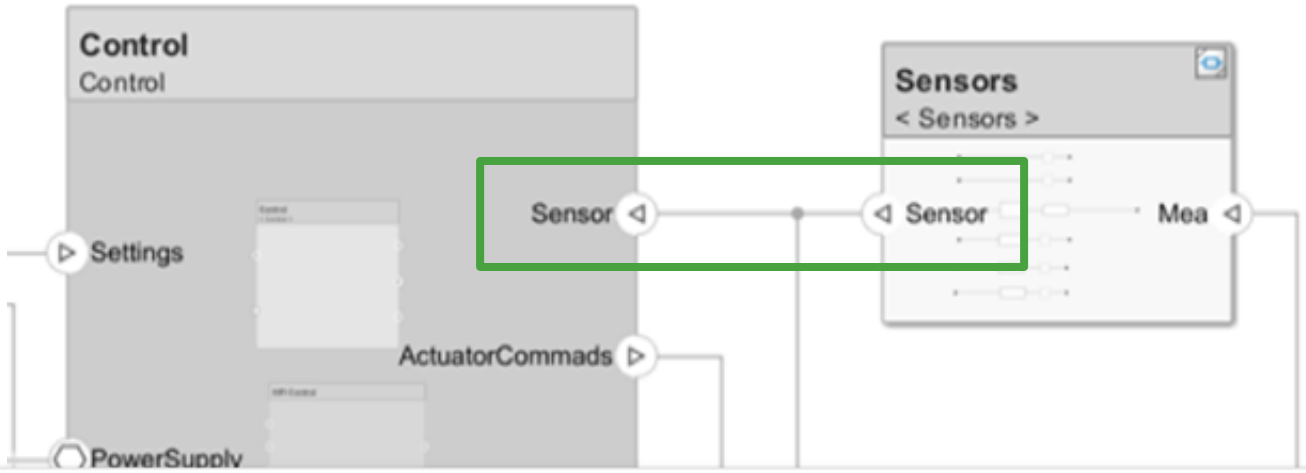
Adding models to your System Engineering

Components

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



Adding models to your System Engineering

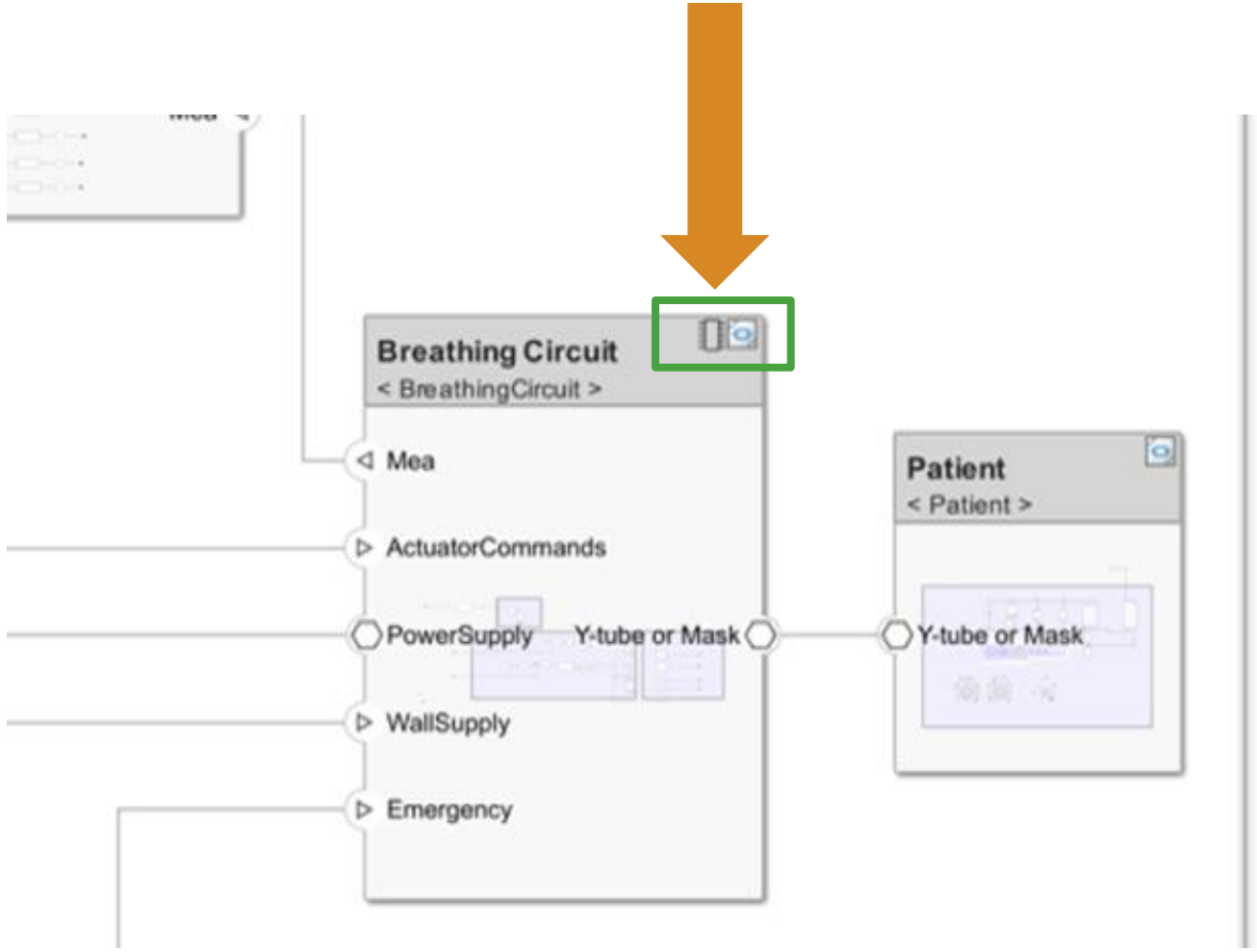


Sensor						
InspPressure	double	1	mbar	real	0	100
ExpPressure	double	1	mbar	real	0	50
InspFlow	double	1	l/min	real	0	180
ExpFlow	double	1	l/min	real	0	300
O2_Fraction	double	1	1	real	21	100
ProximalPressure	double	1	mbar	real	[]	[]
ProximalPressureEsstm	double	1	mbar	real	[]	[]

Adding models to your System Engineering

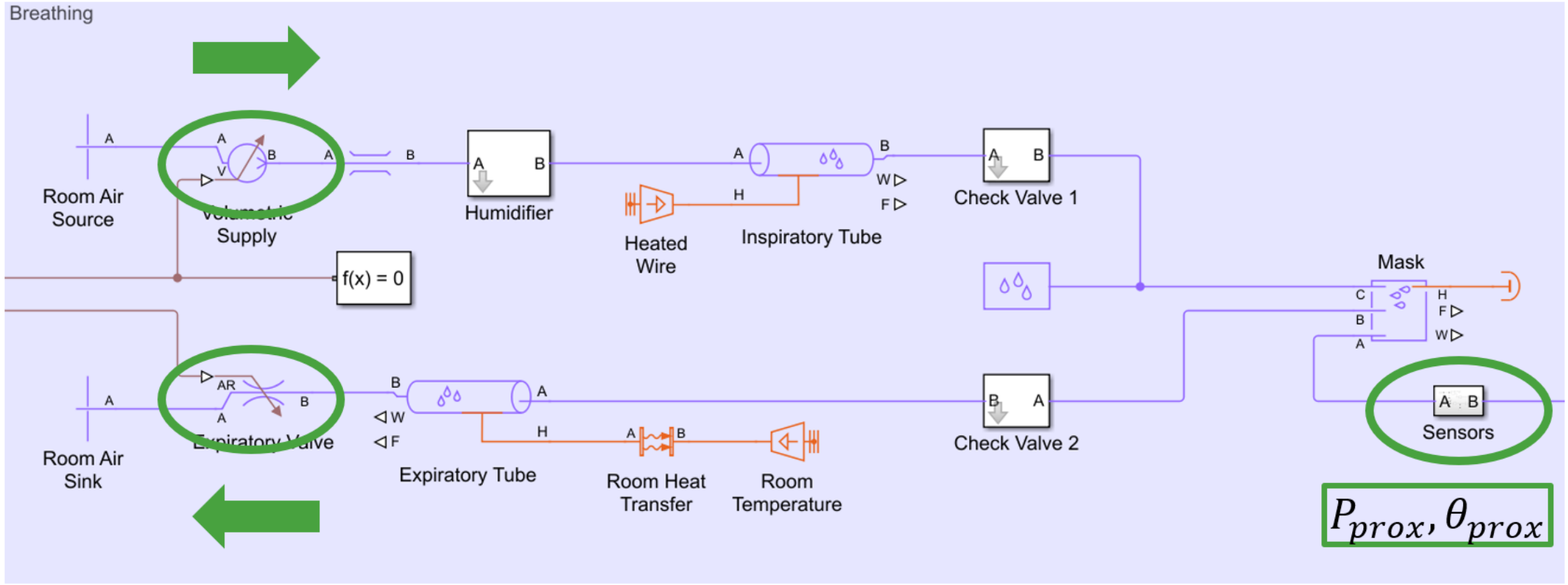
Components

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



Adding models to your System Engineering

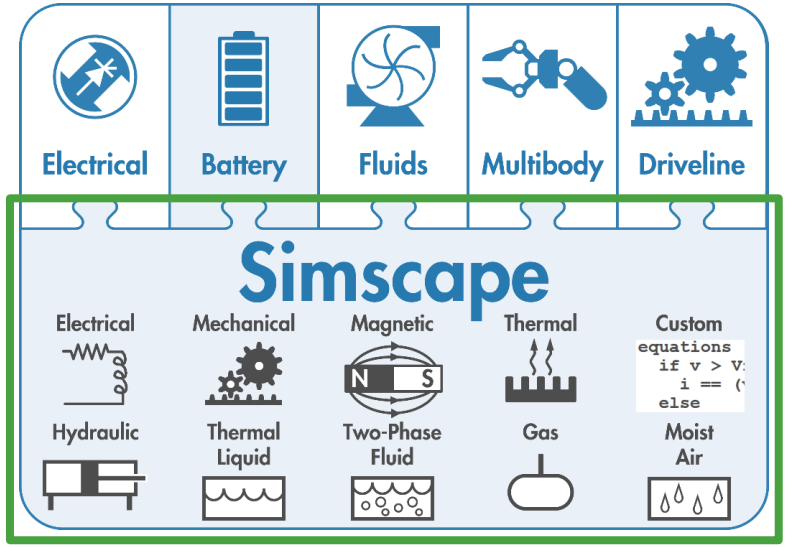
P_{insp}, θ_{insp}

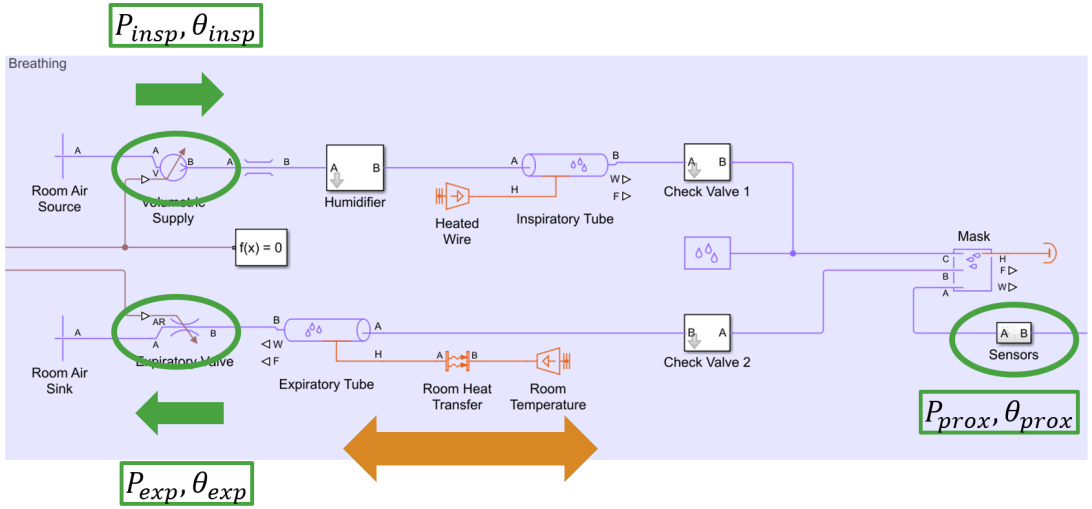


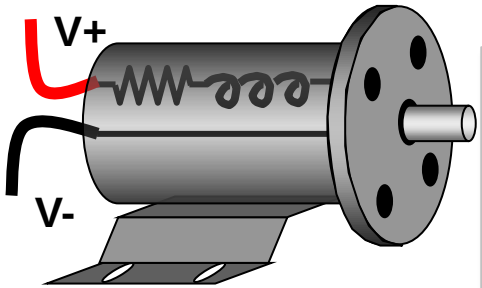
P_{prox}, θ_{prox}

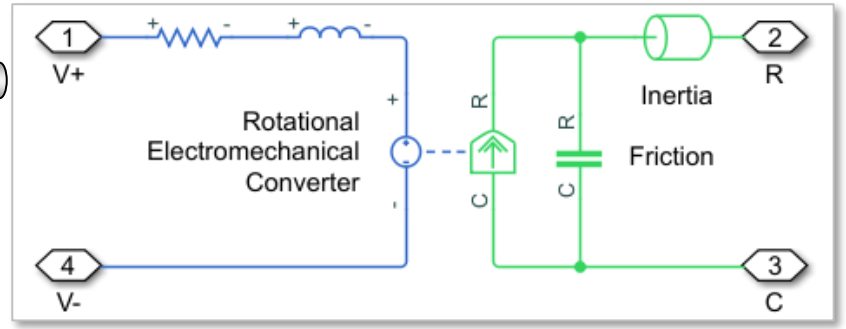
P_{exp}, θ_{exp}

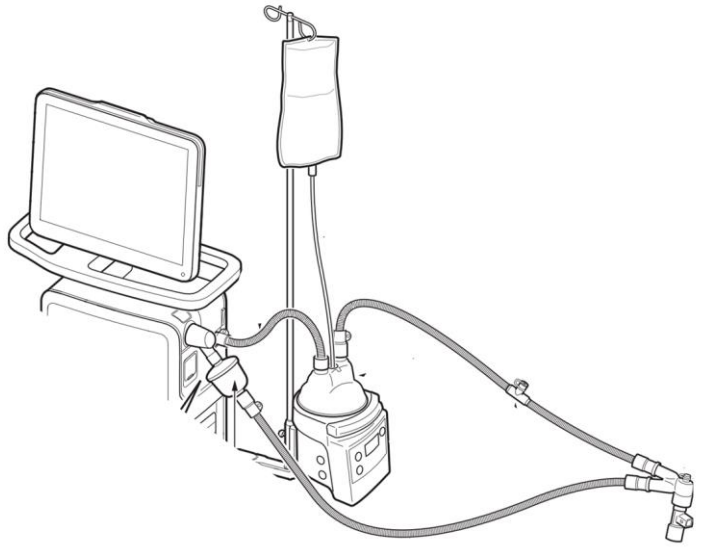
Adding models to your System Engineering



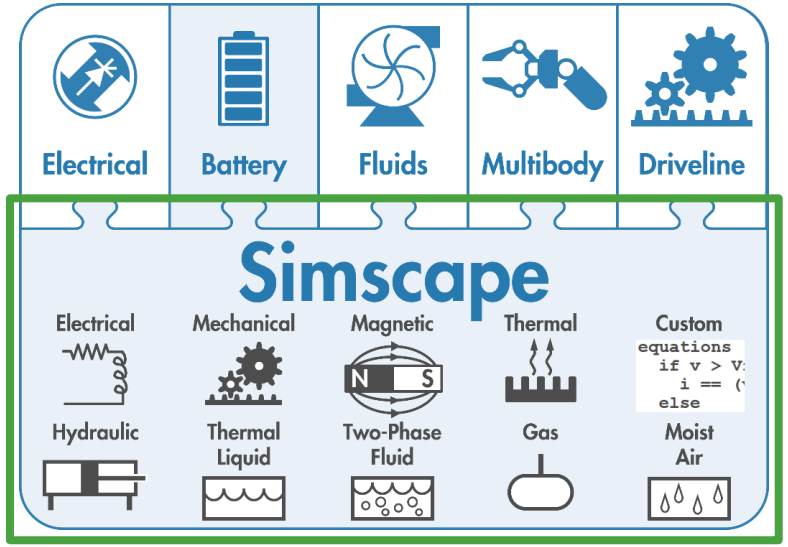


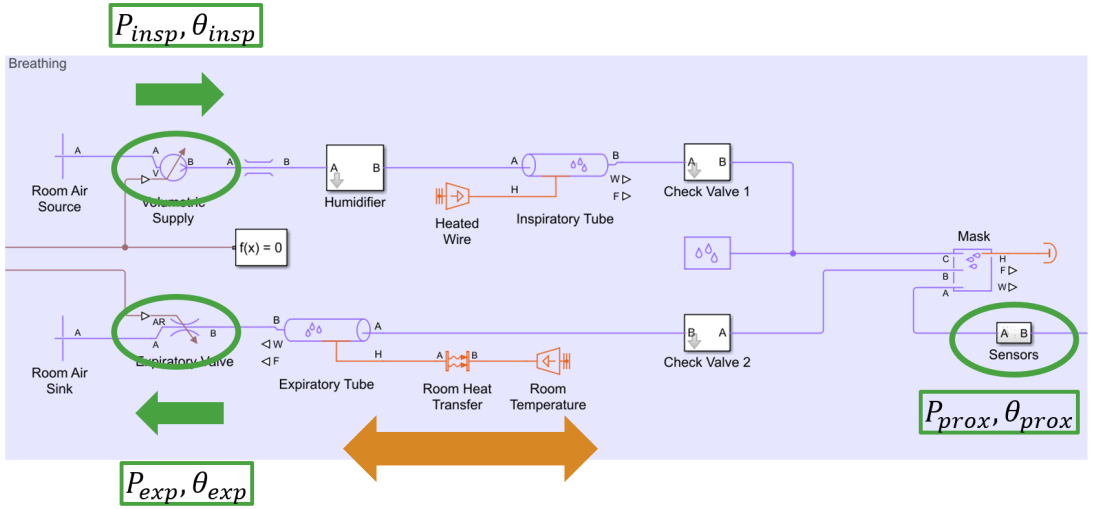




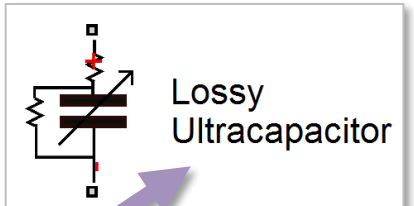


Adding models to your System Engineering



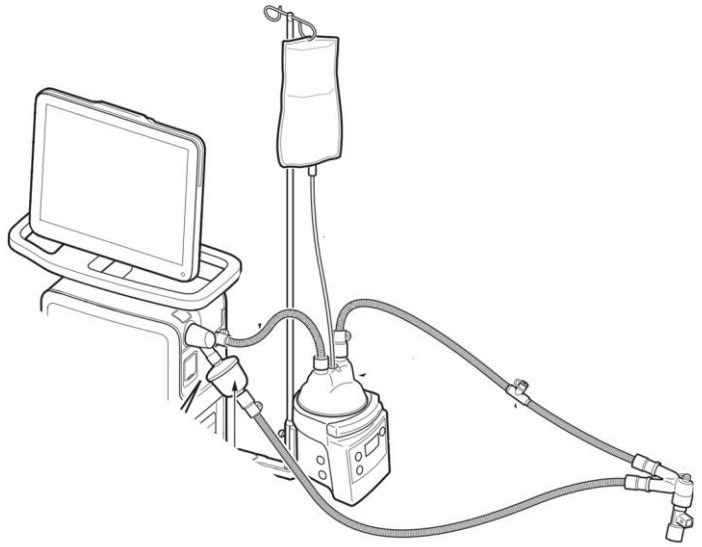


$$i = (C_0 + C_v v)\frac{dv}{dt} + \frac{v}{r_d}$$

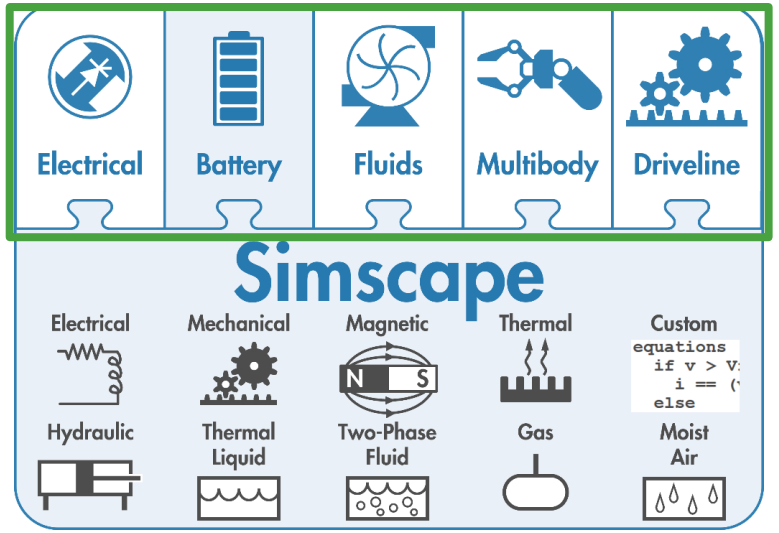


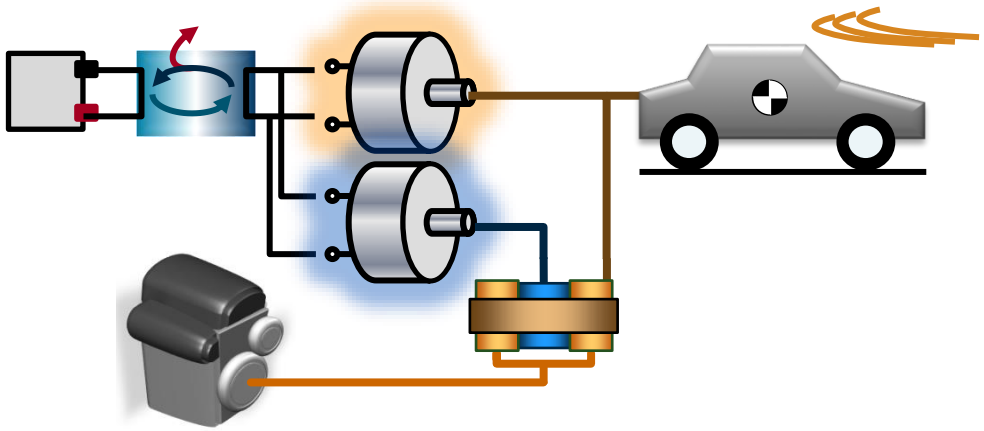
Lossy Ultracapacitor

```
Editor - C:\+MyComponents\LossyUltraCapacitor.ssc
40  equations
41    i == (C0 + Cv*vc)*vc.der + vc/Rd;
42    v == vc + i*R;
43  end
```

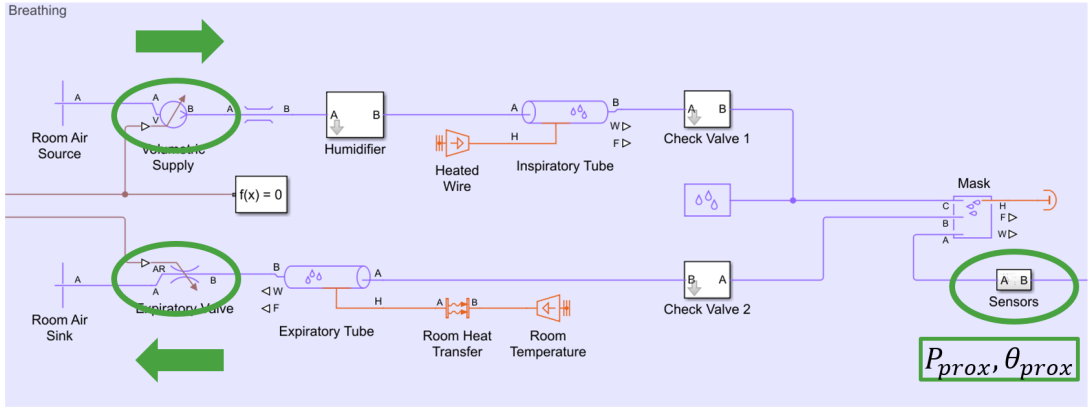


Adding models to your System Engineering





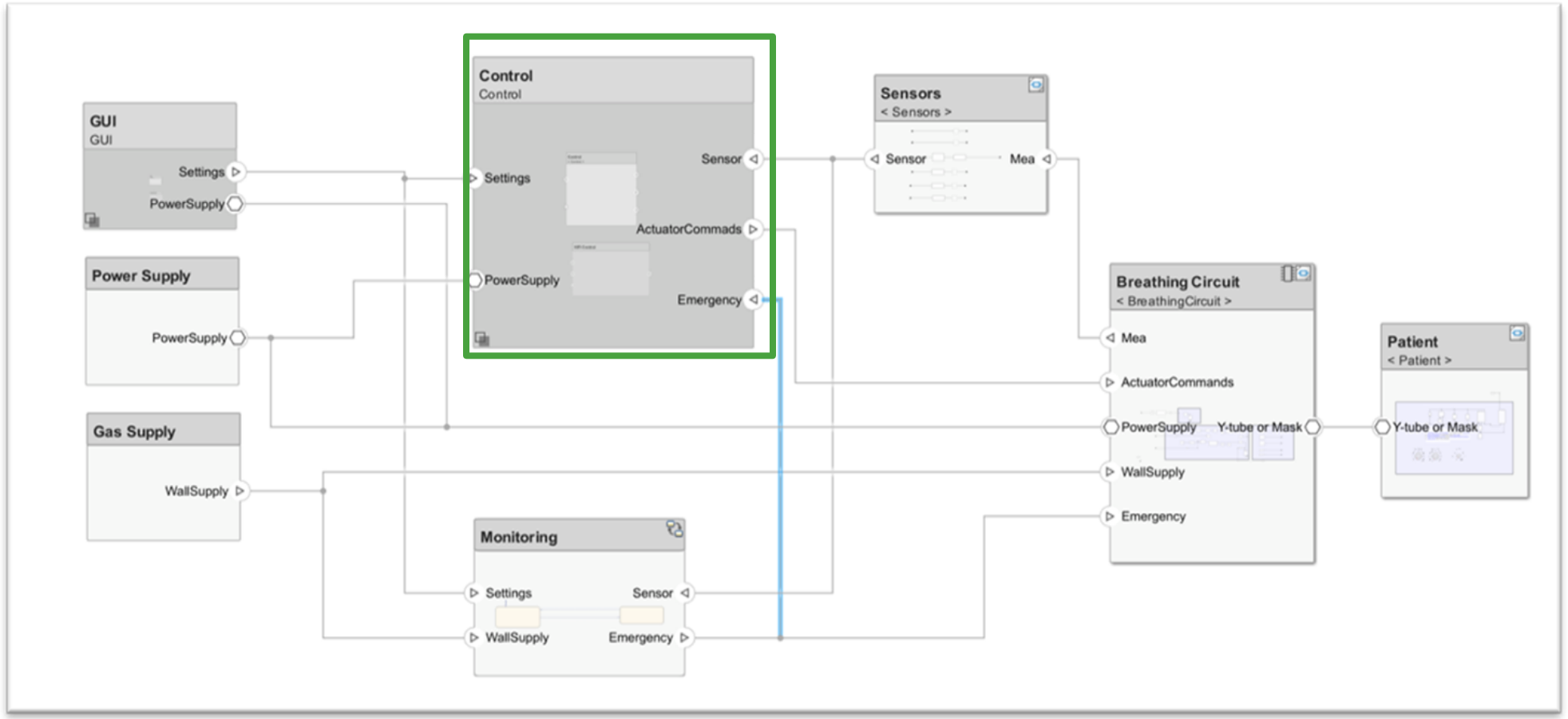
P_{insp}, θ_{insp}



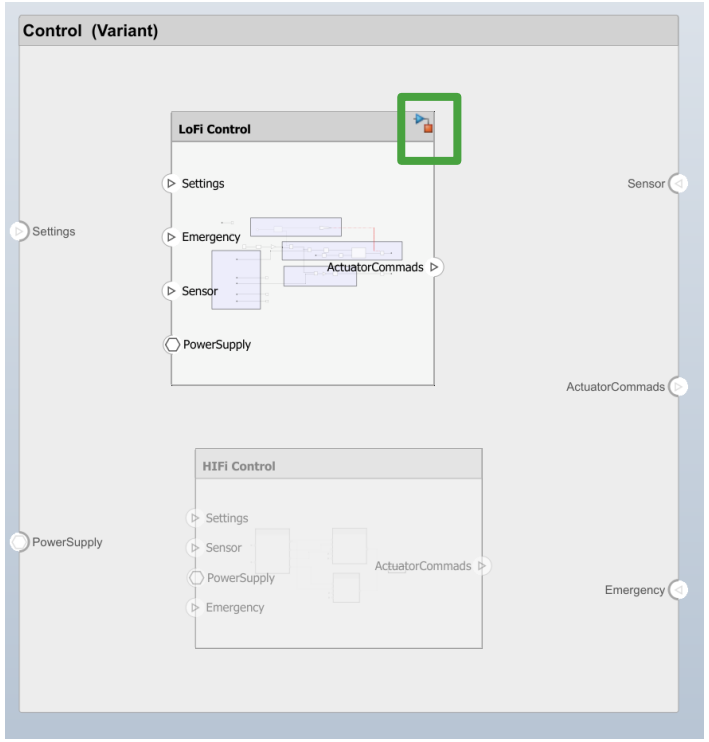
P_{prox}, θ_{prox}

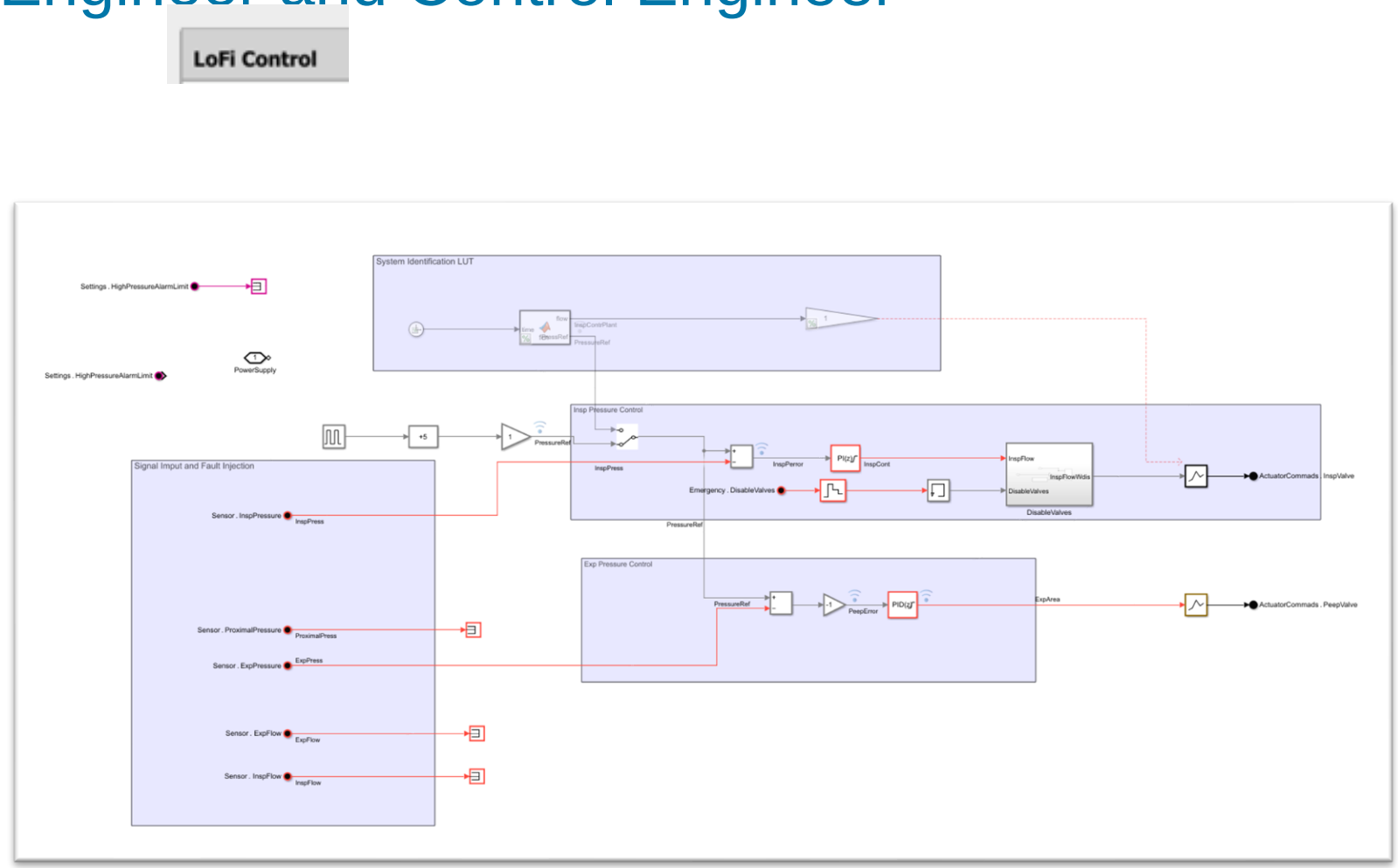
P_{exp}, θ_{exp}

Collaboration: System Engineer and Control Engineer

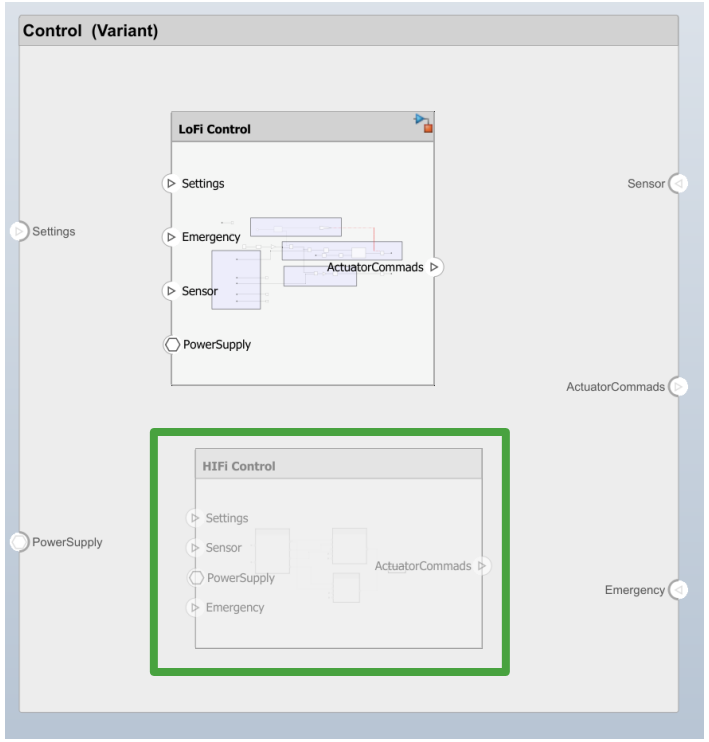


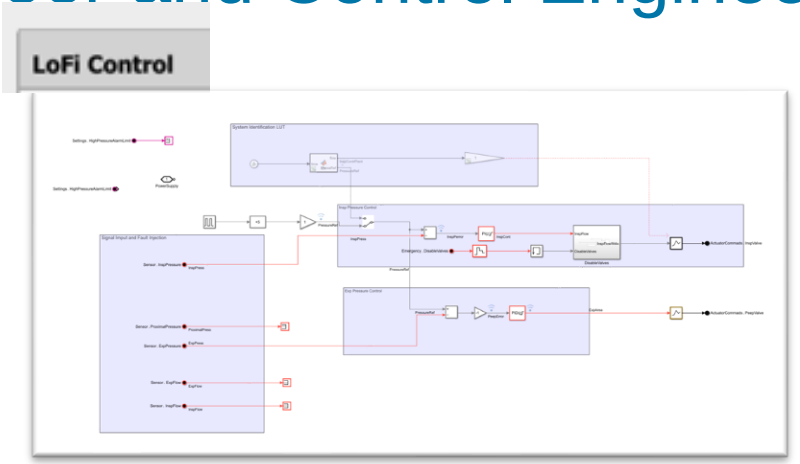
Collaboration: System Engineer and Control Engineer

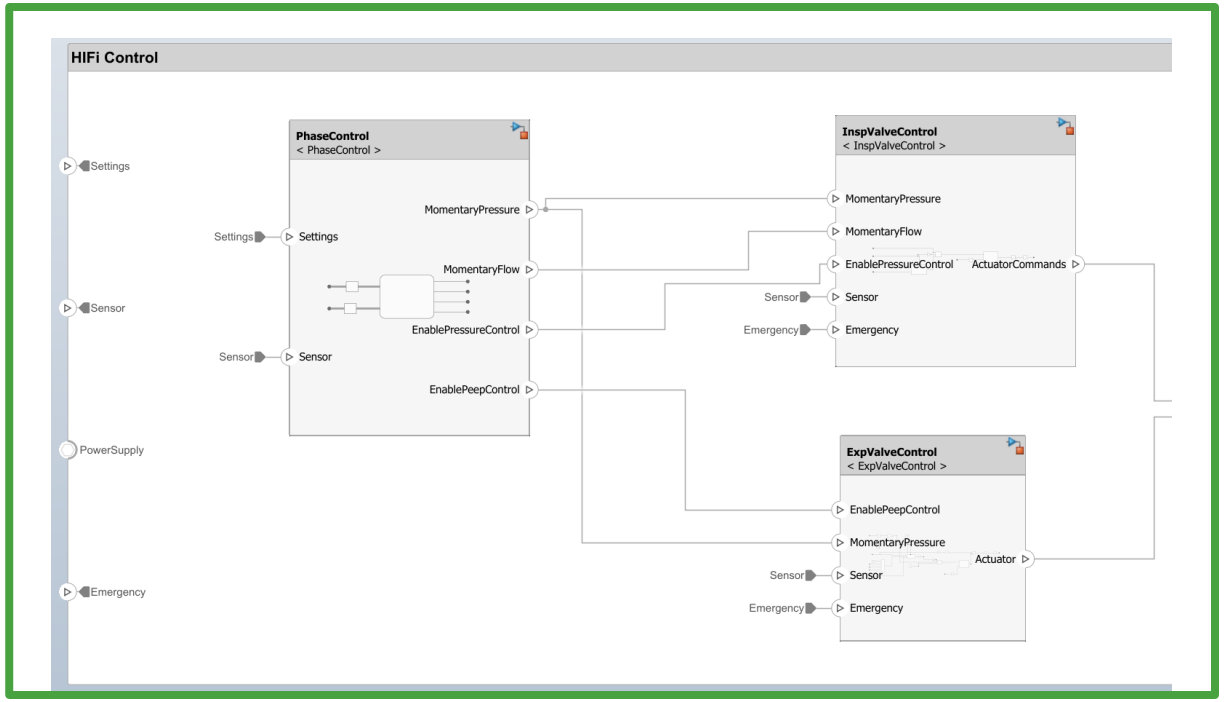




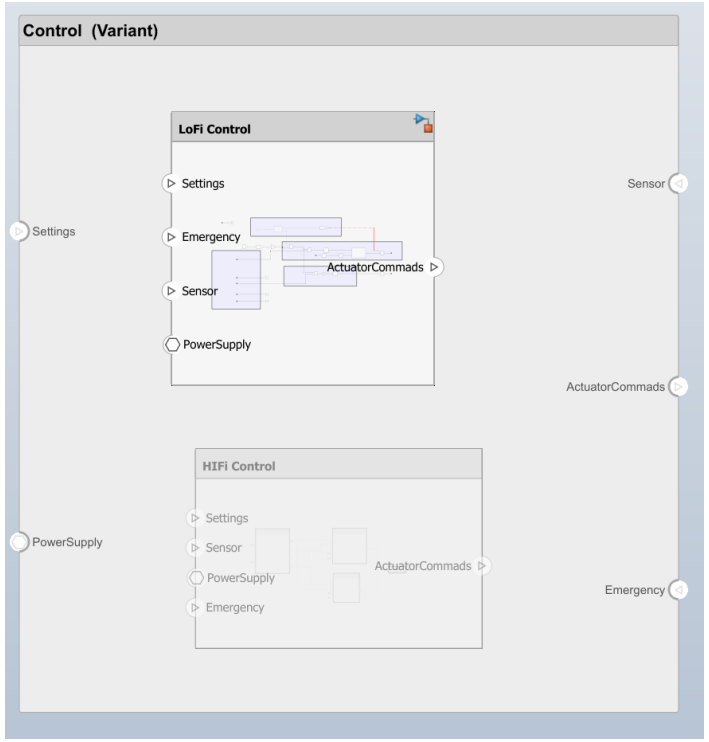
Collaboration: System Engineer and Control Engineer

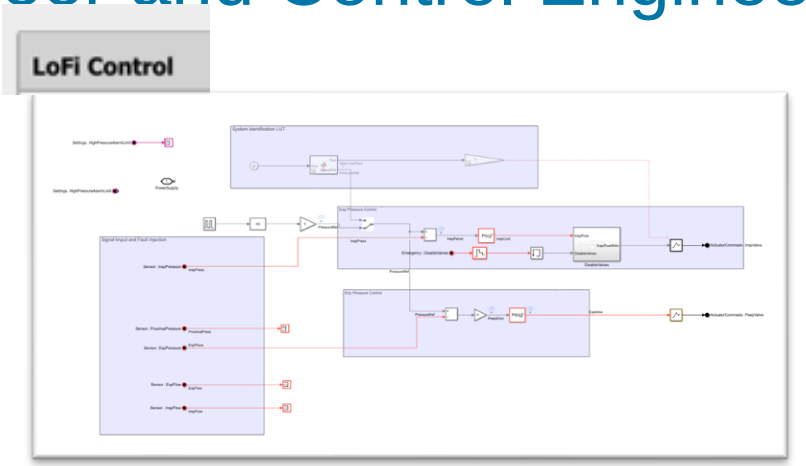


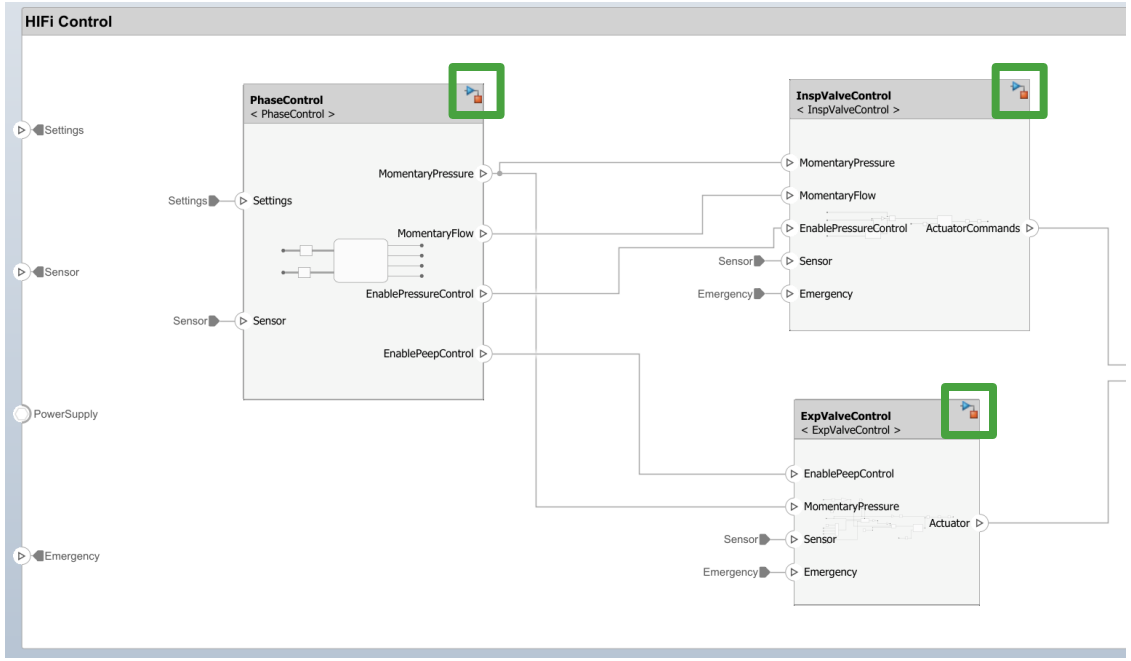




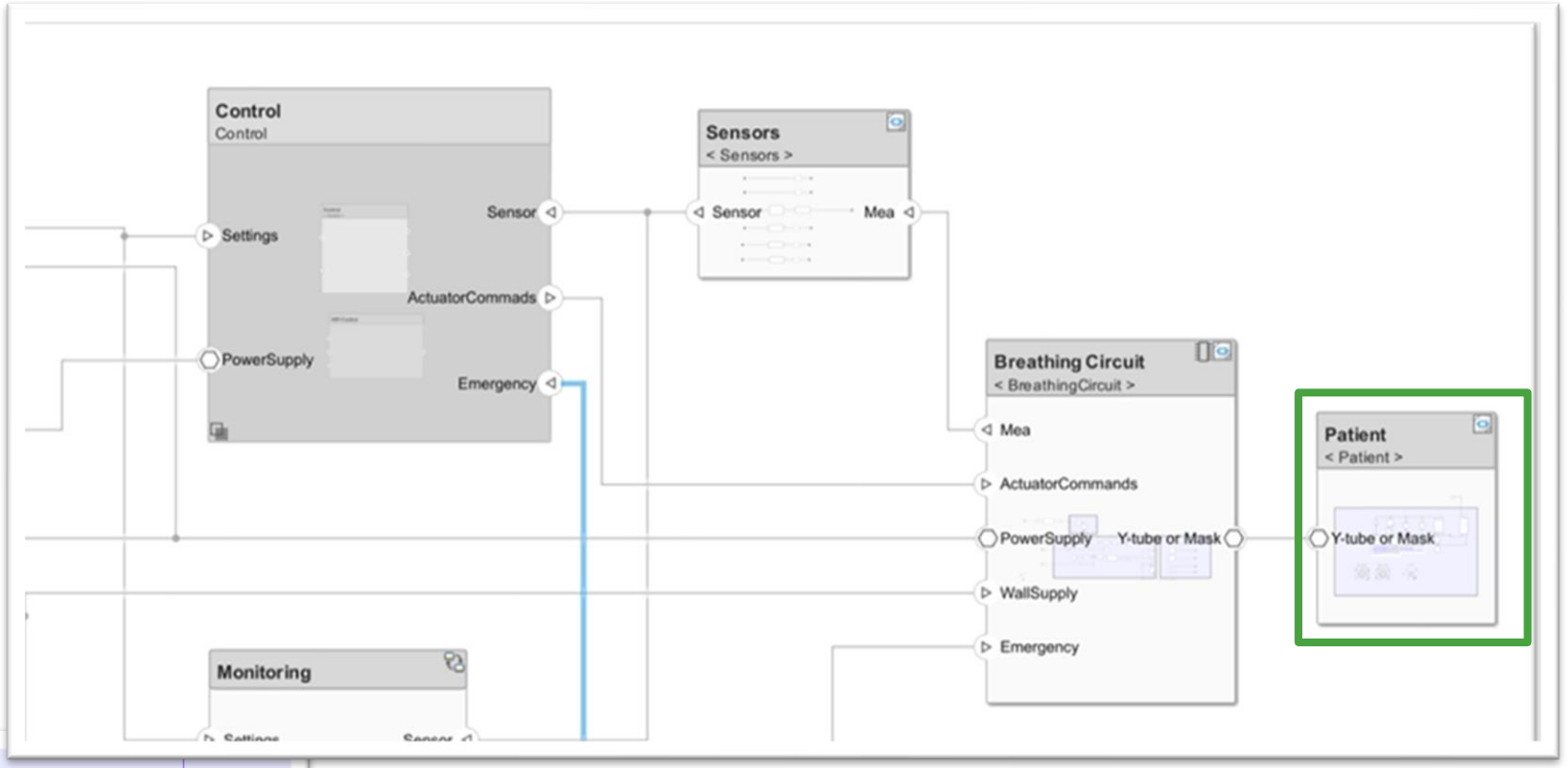
Collaboration: System Engineer and Control Engineer

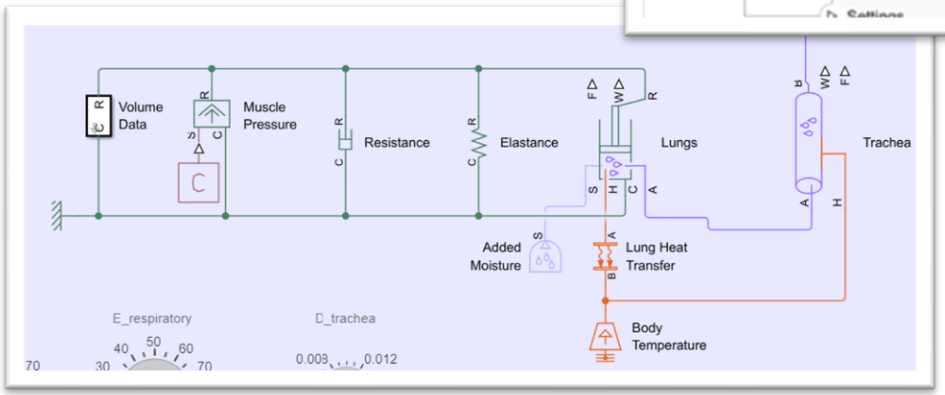




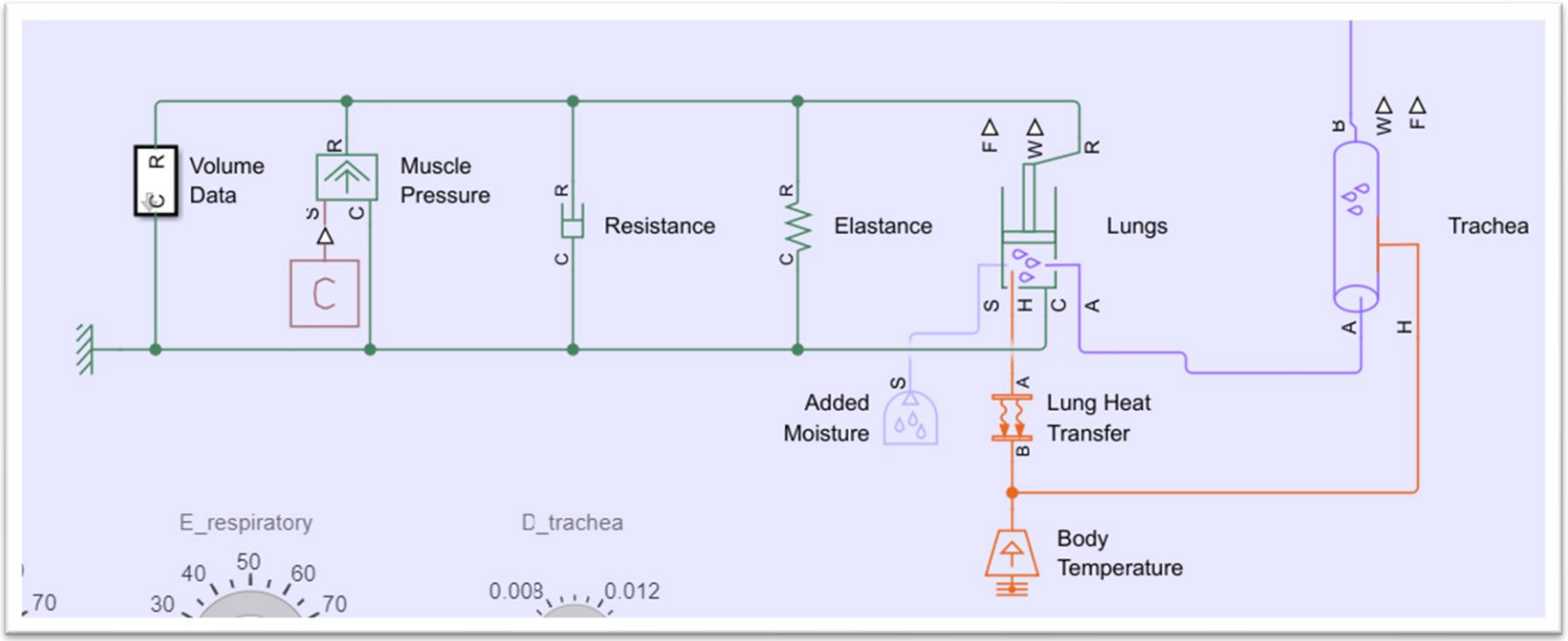


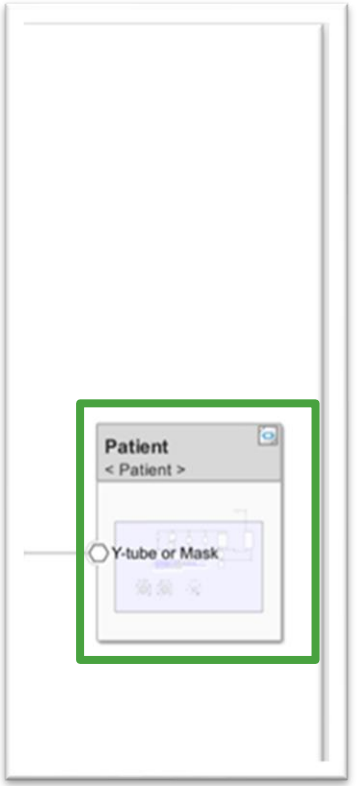
Collaboration: System Engineer and Control Engineer



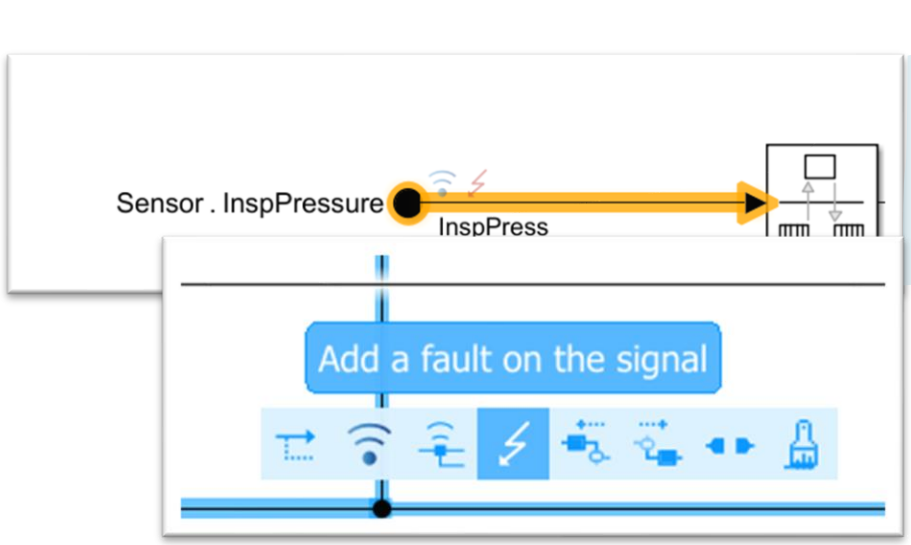


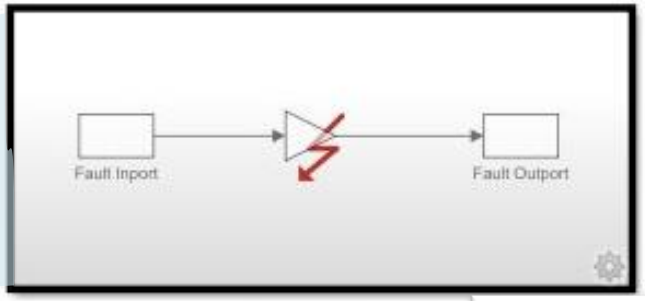
Collaboration: System Engineer and Control Engineer



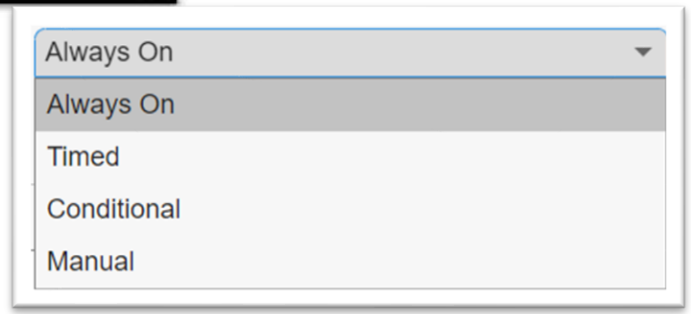


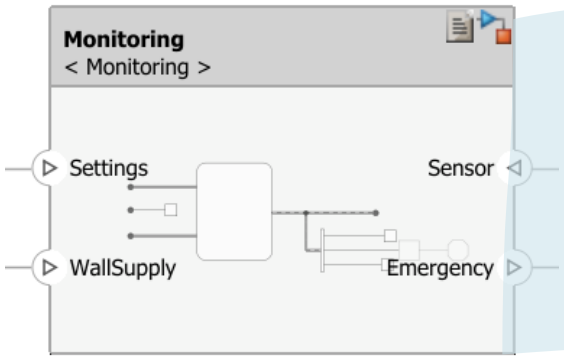
Injecting Errors and detection method

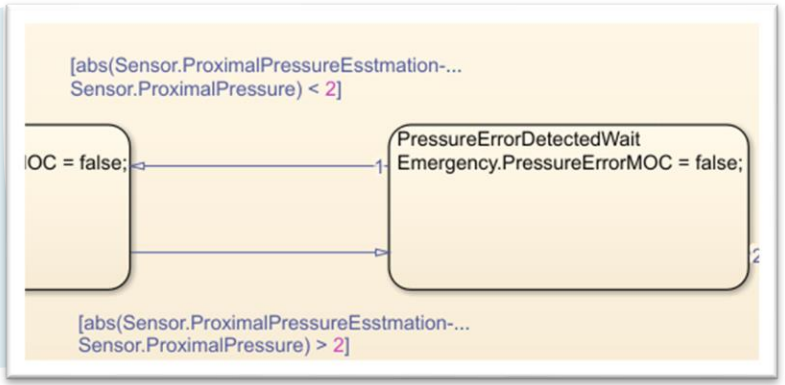




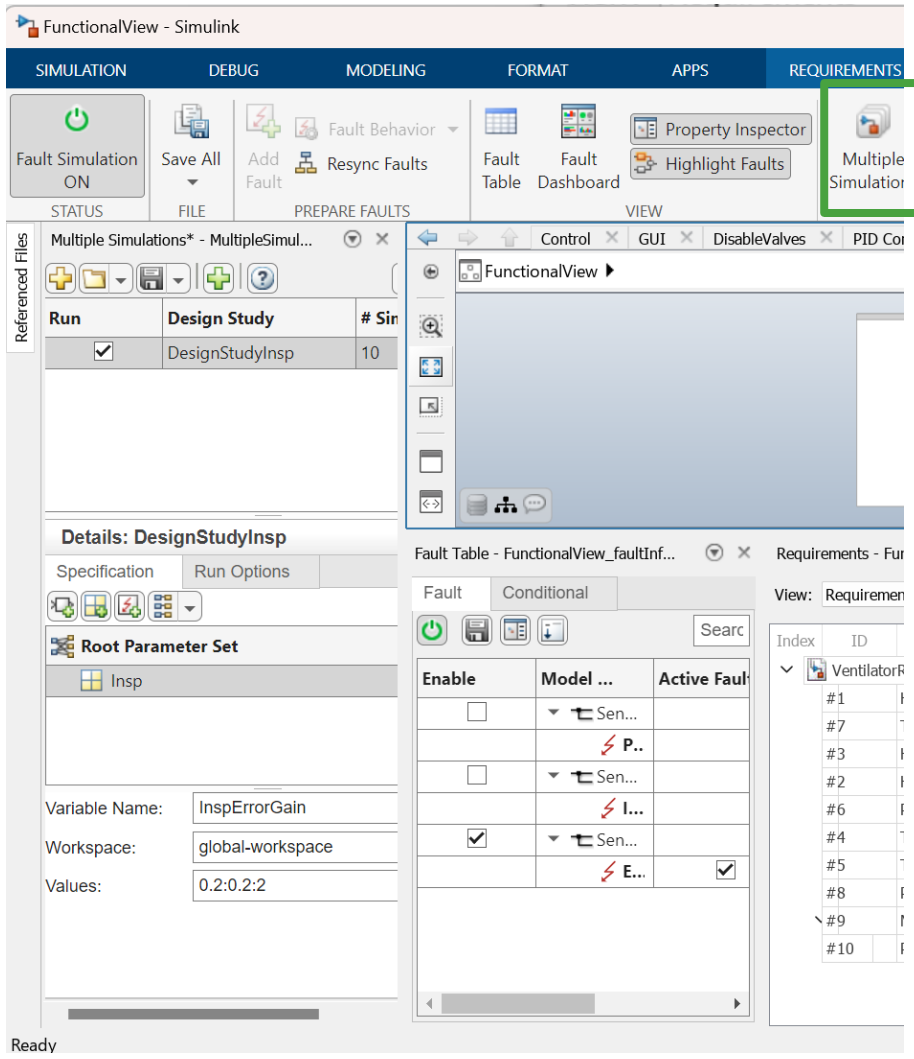
gain_fault

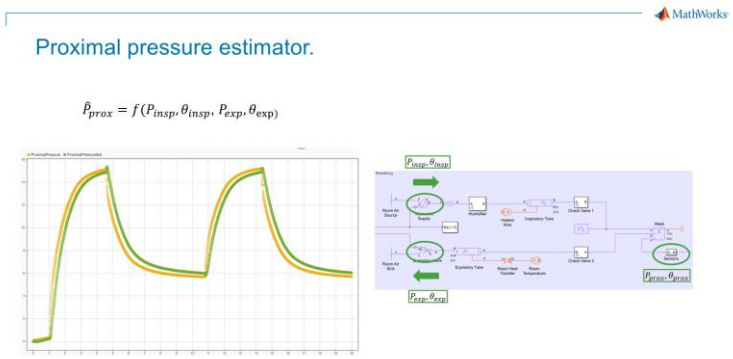


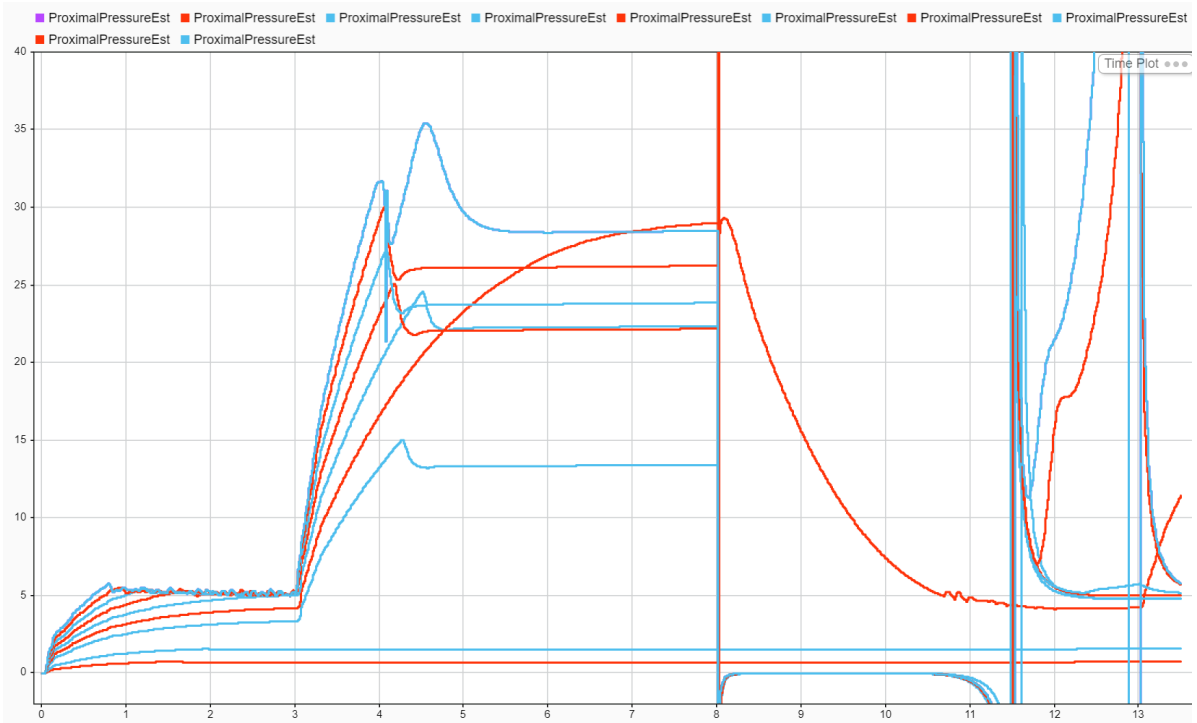




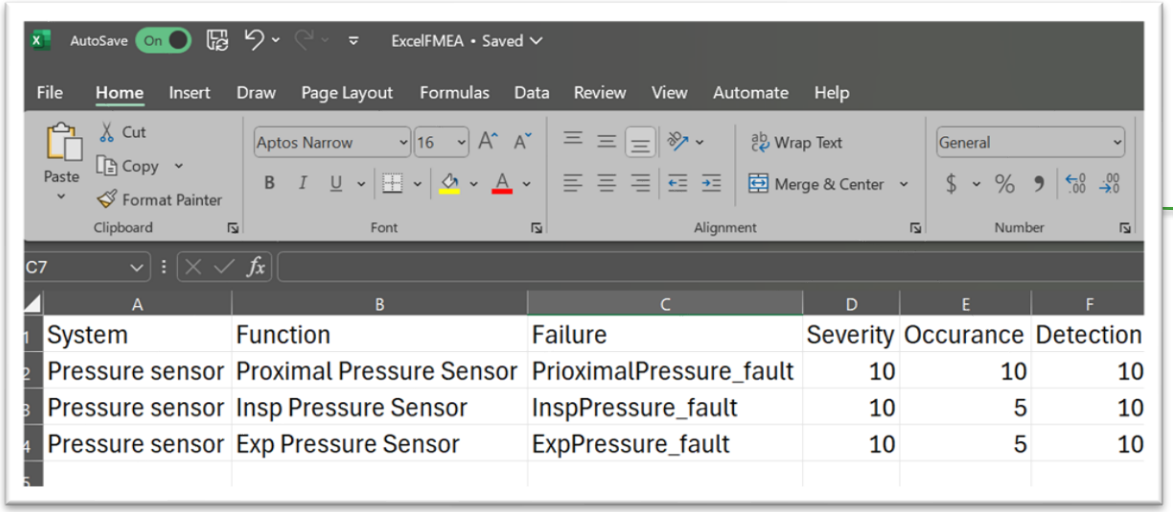
Fast, complete, and parallel verification
Design Study

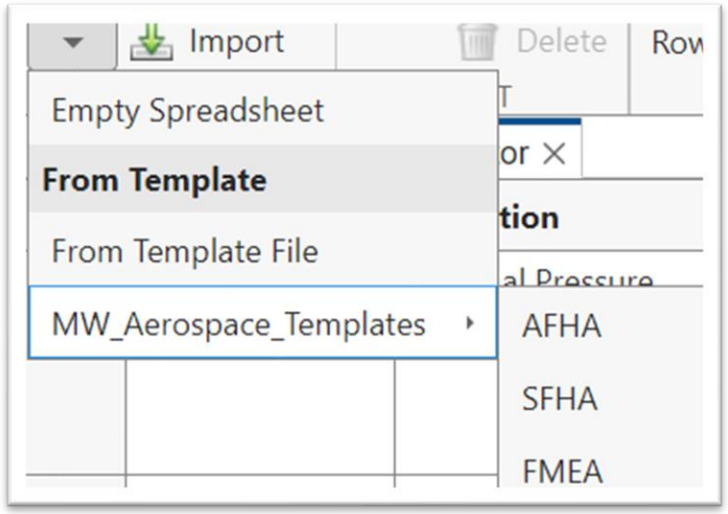


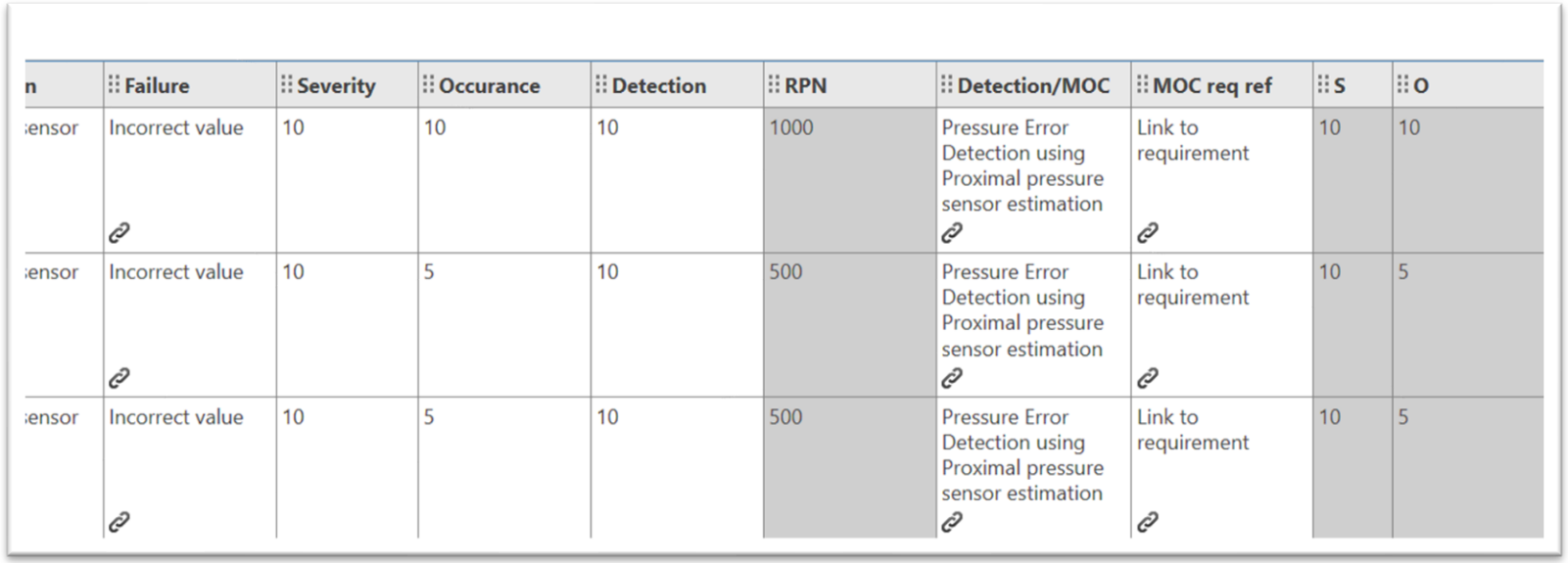




Import FMEA in Excel to Simulink



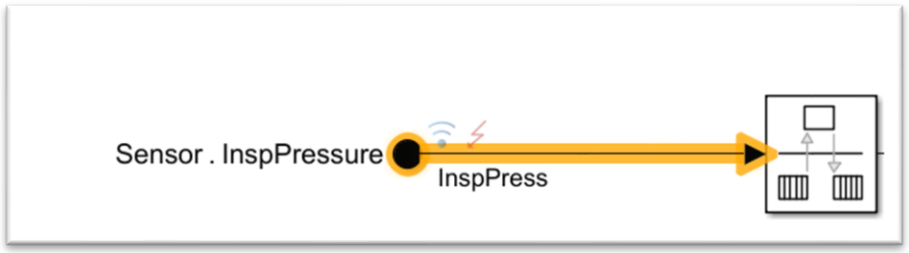


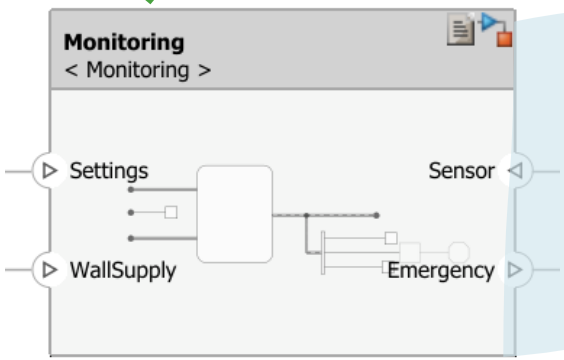


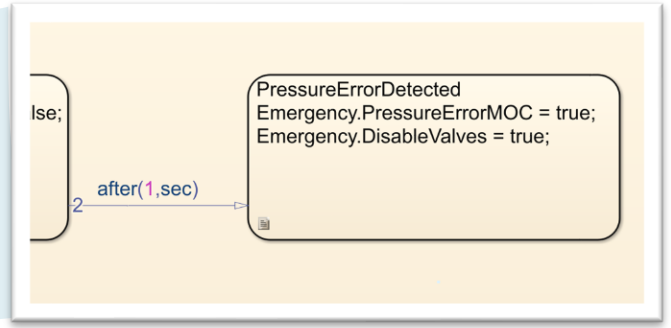
n	Failure	Severity	Occurance	Detection	RPN	Detection/MOC	MOC req ref	S	O
ensor	Incorrect value	10	10	10	1000	Pressure Error Detection using Proximal pressure sensor estimation	Link to requirement	10	10
ensor	Incorrect value	10	5	10	500	Pressure Error Detection using Proximal pressure sensor estimation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

on	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 e	10	5	10	500	Pressu rror Detec using Proxin ressure sensor mation	Link to requirement	10	5
sensor	Incorrect v	10	5	10	500	Pressur or Detecti sing Proxima ssure sensor e ation	Link to requirement	10	5

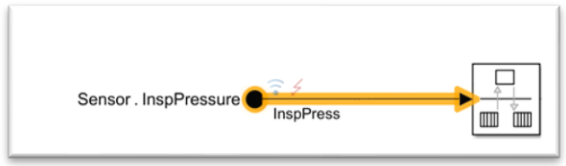


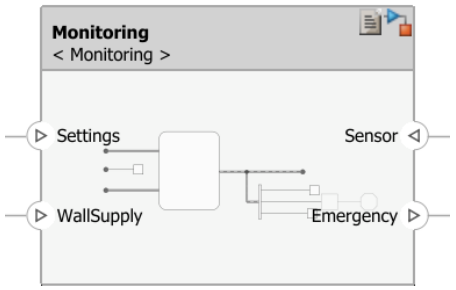


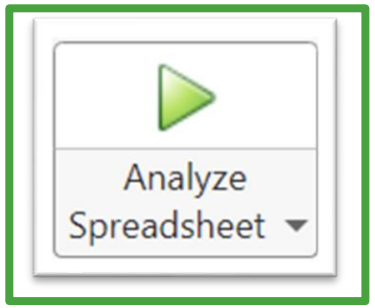


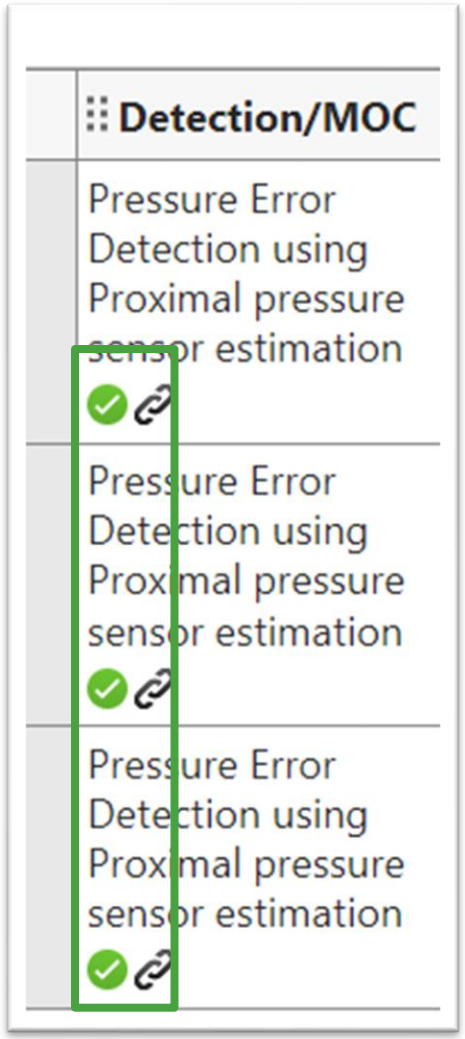
Automatic MOC verification

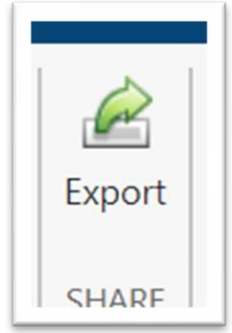
on	Failure	Severity	Occurance	Detection	RPN	Detection/MOC	MOC req ref	S	O
sensor	Incorrect value	10	10	10	1000	Pressure Error Detection using Proximal pressure sensor estimation	Link to requirement	10	10
sensor	Incorrect va	10	5	10	500	Pre Error De n using P al pressure r estimation	Link to requirement	10	5
sensor	Incorrect valu	10	5	10	500	essure Error Detection using Proximal pressure sensor estimation	Link to requirement	10	5



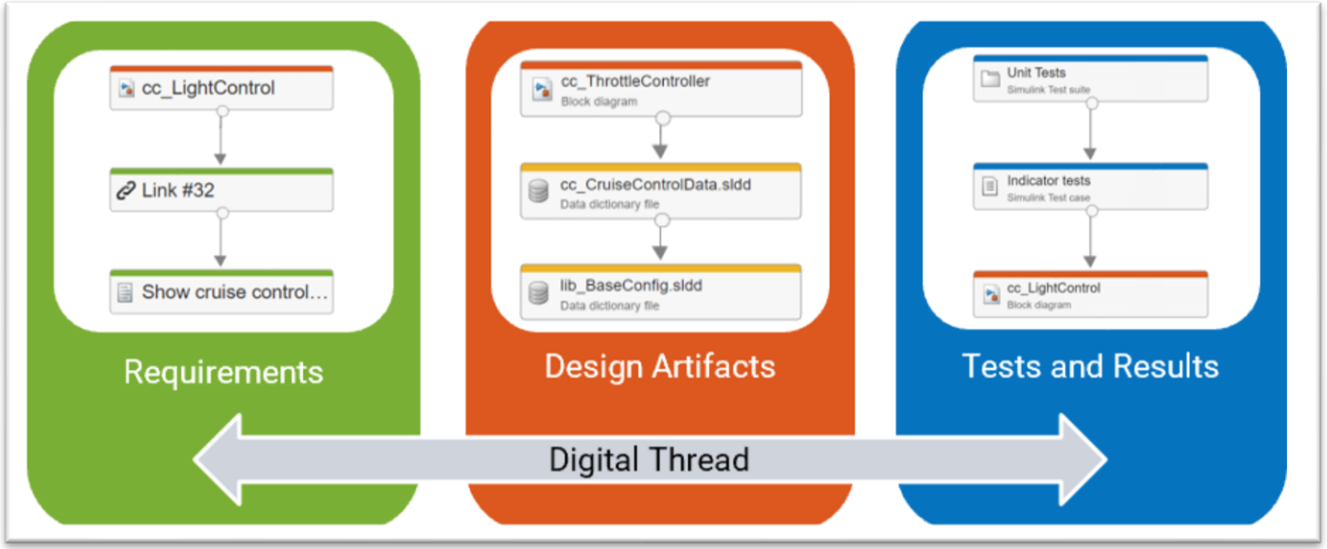








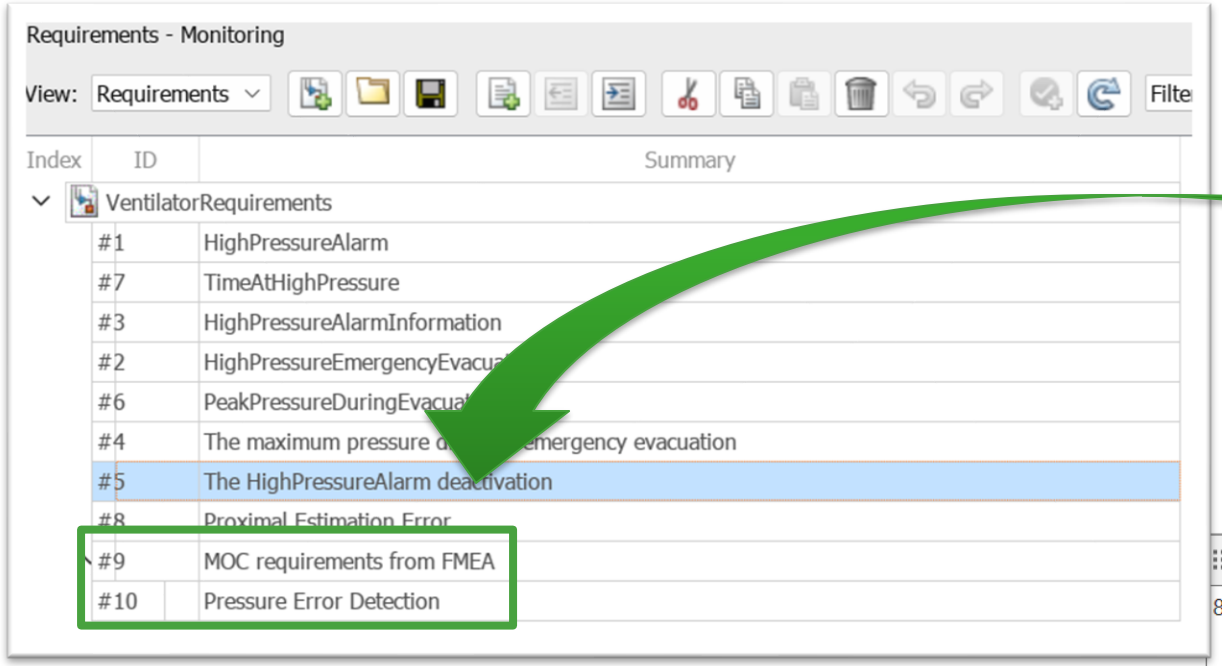
Digital Thread



xtended ×

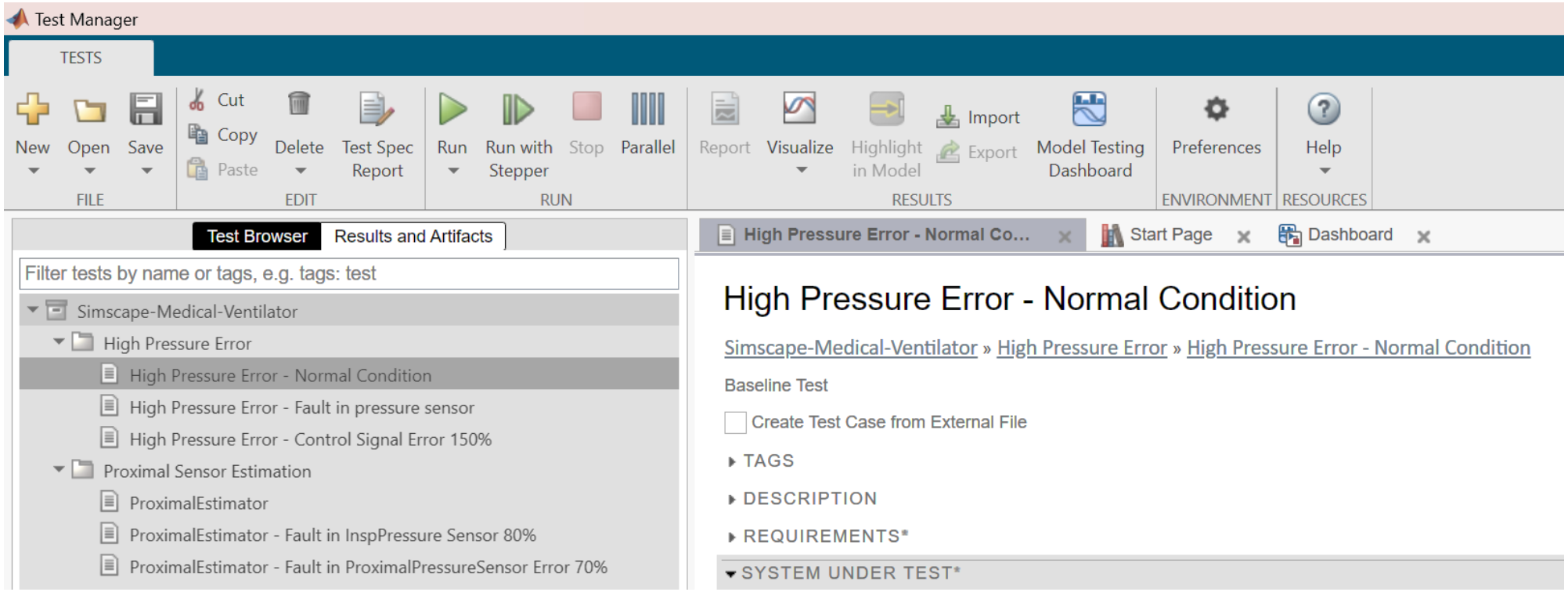
	Failure	Local Effect	System Effect	S	Po	Detection	RPN	Detection/MOC	MOC req ref
re	Incorrect value	Incorrect pressure control. Higher true pressure if control pressure is falsly lower.	Possible barotrauma.	8	8	10	640	Pressure Error Detection using Proximal pressure sensor estimation	When pressure error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

Digital Thread

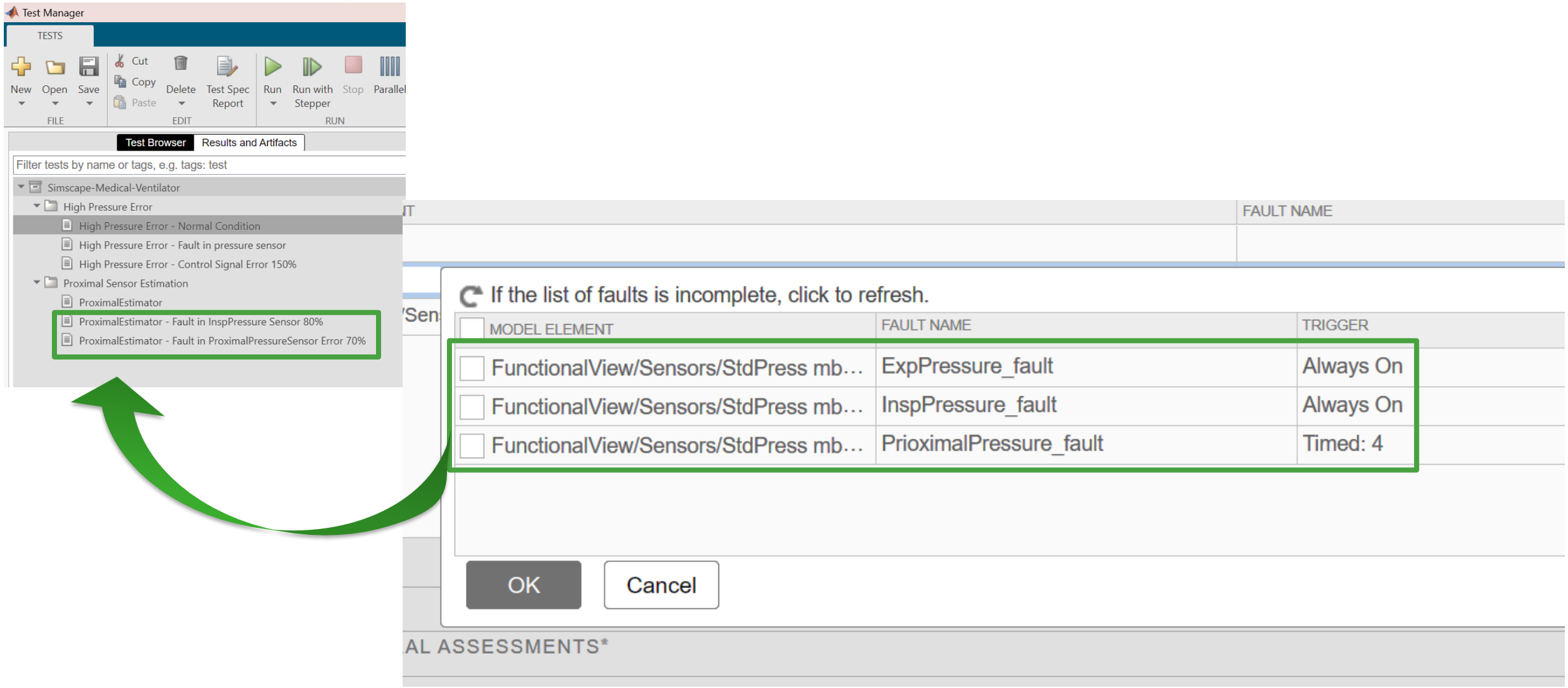


Po	Detection	RPN	Detection/MOC	MOC req ref
8	10	640	Pressure Error Detection using Proximal pressure sensor estimation	When pressure error is detected the disable valves shall be set to true, stopping ventilation and activate high level alarm.
5	10	400	Pressure Error Detection using Proximal pressure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

Collaboration: System Engineer and Test Engineer Reuse of Faults



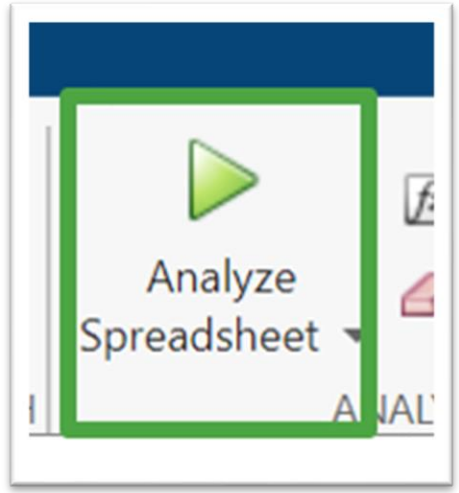
Collaboration: System Engineer and Test Engineer
Reuse of Faults



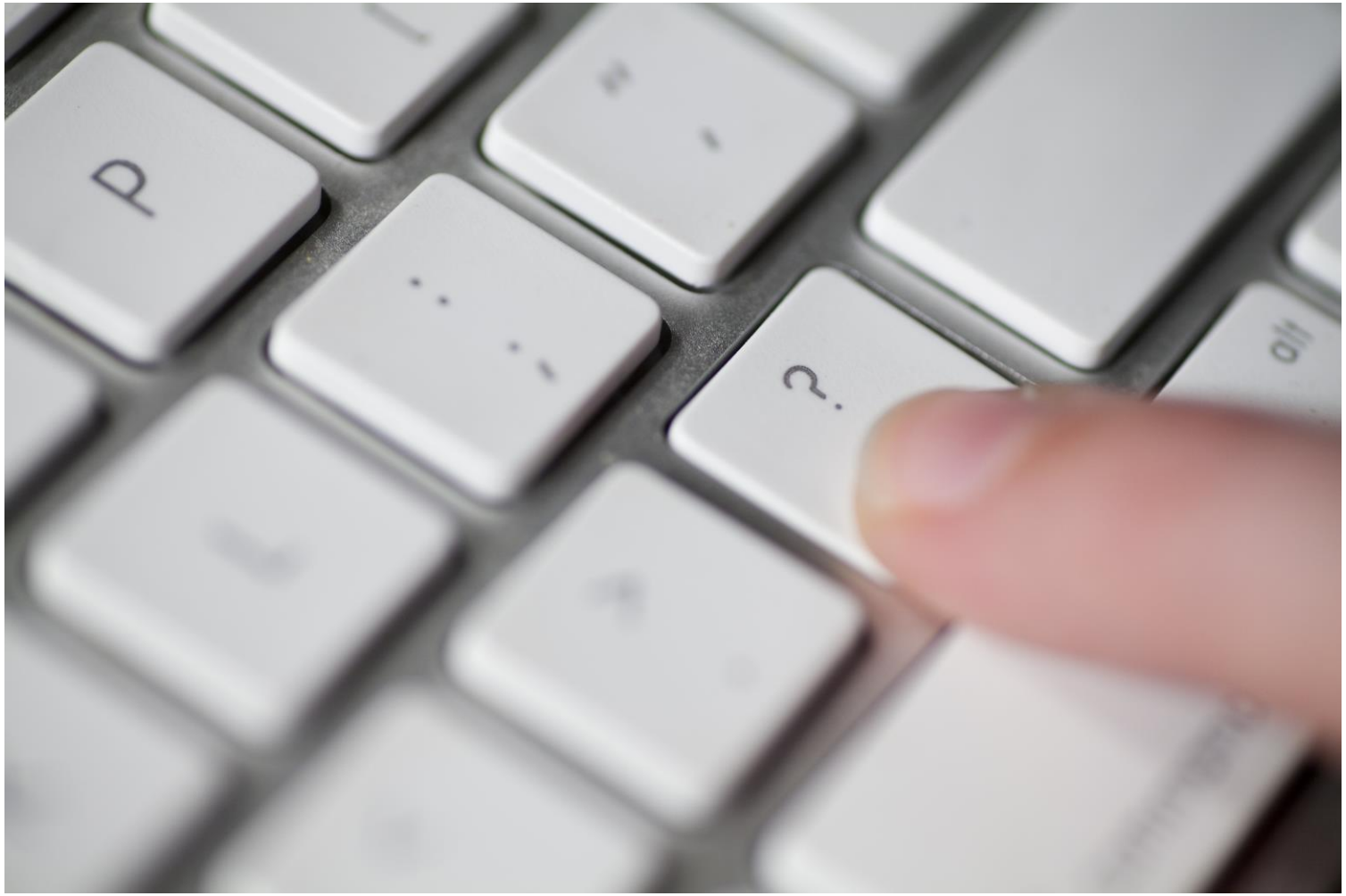
Another great reason to automate your FMEA

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

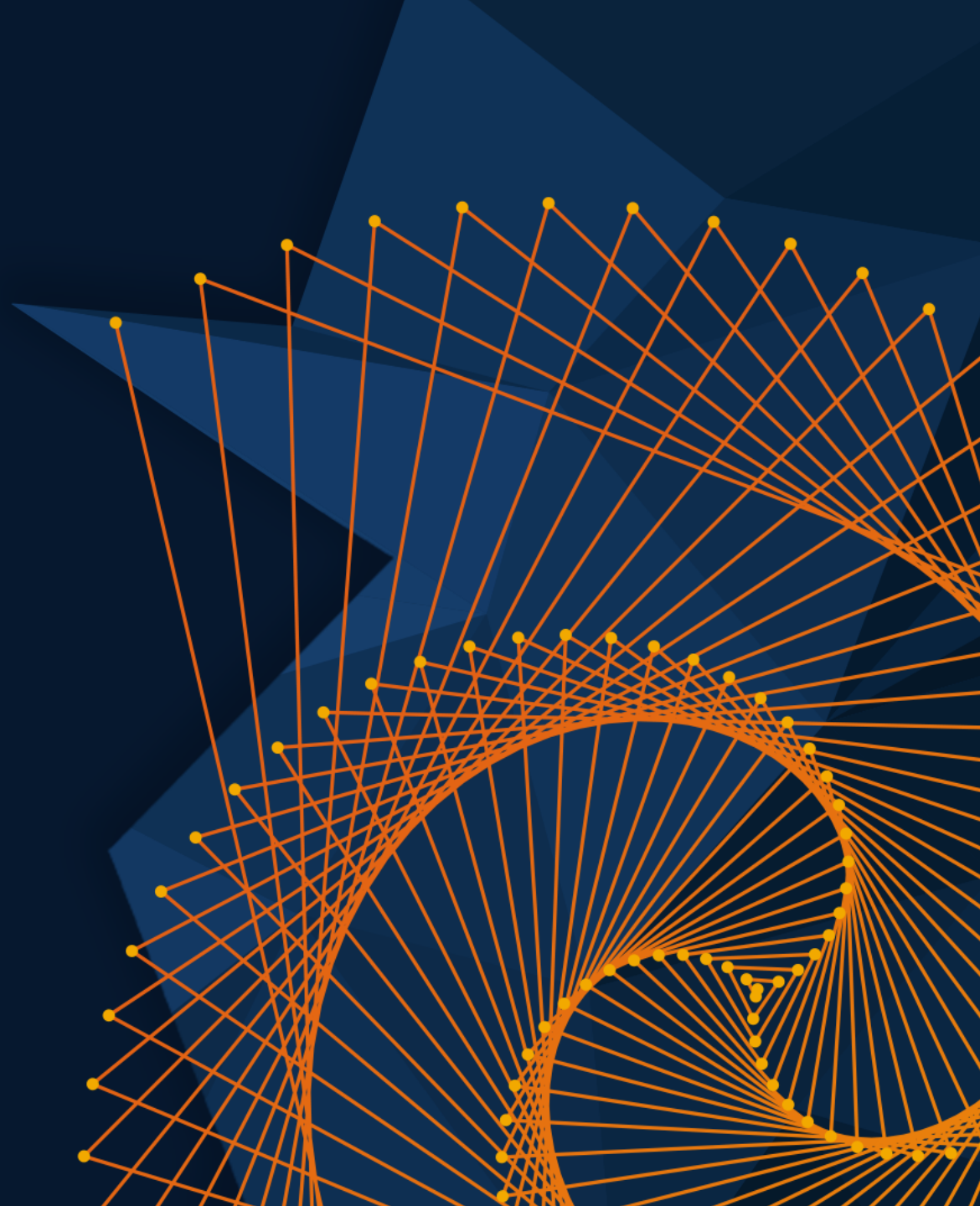


Questions?



MATLAB EXPO

FRANCE



MathWorks®