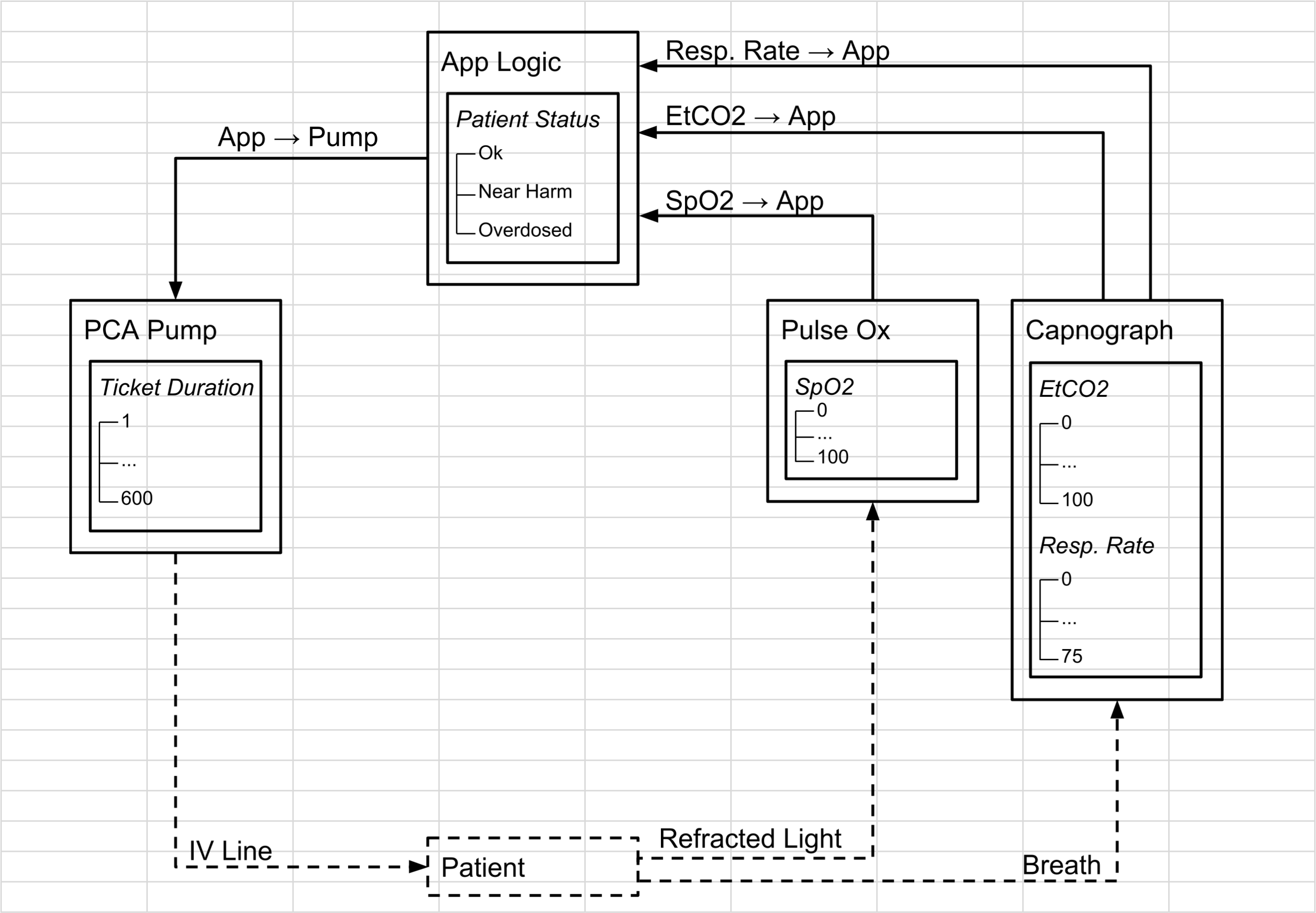
System:	PCA Interlock								**System Boundary**	
	Fundamentals								System	Environment
	Name	Reference							PCA Pump	Patient
									App Logic	
Accident Levels:	AL. DeathOrSeriousInjury	N / A							Pulse Oximeter	
									Capnograph	
Accidents:	Acc. PatientHarmed	AL. DeathOrSeriousInjury								
			Hazardous Factor	System Element	System Element State	Env. Element	Env. Element State			
Hazards:	H. TooMuchAnalgesic	Acc. PatientHarmed	Analgesic	PCA Pump	Pumping	Patient	NearHarm			
Safety Constraints:	SC. DontODPatient	H. TooMuchAnalgesic								
Explanations										
Reference	Explanation									
Acc. PatientHarmed	The patient is harmed or seriously injured as a result of the App's actions									
H. TooMuchAnalgesic	The patient is given more analgesic than they can safely tolerate									
Architecture	As modeled by Arney-etal in ICCPS10 (in section 4.3) with some modifications									
	A lot of possibly unmeetable assumptions (guaranteed timing of network and app)									
	Modified to include RR and EtCO2 physiological monitors (in addition to SpO2)									



App Logic
Patient Status
Ok
Near Harm
Overdosed
Resp. Rate → App
EtCO2 → App
SpO2 → App
App → Pump
PCA Pump
Ticket Duration
1
...
600
Pulse Ox
SpO2
0
...
100
Capnograph
EtCO2
0
...
100
Resp. Rate
0
...
75
IV Line
Patient
Refracted Light
Breath

Activity 0: Fundamentals

Step 0.2

Element:	Successor Link Name:	Predecessor Link Name(s)	Classification	
PCA Pump	PCA Pump -> IV Line	AppLogicCommands -> PCA Pump	**Architectural:**	Actuator

Activity 1: Unsafe Interactions

Step 1.1	**Step 1.2**						
	Manifestations						
Successor Dangers	**Pred. Link**	**Content**		**Halted**	**Erratic**	**Timing**	
		High	Low			Early	Late
SC.DontODPatient	AppLogicCommands -> PCA Pump	PCAPump. TicketTooLong	Not Hazardous	Not Hazardous	PCAPump. ErraticTicket	PCAPump. EarlyTicket	PCAPump. LateTicket

Process Variable	**Process Values**						**Unit**
Ticket Duration	1	2	3	...	598	599	600	Seconds

Step 1.3

Externally Caused Dangers						**Proposed Mitigations**	
Successor Danger	Name	Process Var. Name	Process Var. Value	Interpretation	Co-occurring Dangers	Run-time Detection	Run-time Handling
SC. DontODPatient	PCAPump. TicketTooLong	Ticket Duration	Higher than safe	The ticket has a time value that is too long	None	None	N / A
SC. DontODPatient	PCAPump. ErraticTicket	Ticket Duration	Any	The PCA Pump gets a ticket "out of the blue"	None	None	N / A
SC. DontODPatient	PCAPump. EarlyTicket	Ticket Duration	Any	The PCA Pump gets a ticket "too soon" -- before it has finished handling the previous ticket	None	Concurrent: Timeouts	Rollforward: Pump switches into permanent KVO (and notifies the clinician?)
SC. DontODPatient	PCAPump. LateTicket	Ticket Duration	Any	The PCA pump gets a ticket late, so it's valid past the time window it should be	None	Concurrent: Timestamped "tickets"	Rollforward: Pump switches into KVO

Activity 2: Internal Faults

Step 2.1

Faults Not Considered

Guideword	Justification
Software Bug	We're using a "proven in use" PCA Pump
Bad Software Design	
Compromised Software	
Compromised Hardware	
Hardware Bug	
Bad Hardware Design	
Production Defect	
Adversary Accesses Hardware	The hospital has physical security measures in place
Adversary Accesses Software	
Syntax Mismatch	The PCA pump isn't a connection between two components
Rate Mismatch	
Semantic Mismatch	

Step 2.2

Internally Caused Dangers

Successor Danger	Guideword	Interpretation	Co-occurring Dangers	Design-time Detection	Run-time Detection	Run-time Error Handling	Run-time Fault Handling

SC. DontODPatient	Deterioration	The pump is poorly maintained and fails open due to deterioration	None	Testing: Maintenance intervals should be established by the manufacturer and verified by regulators	Preemptive: Periodic pump examinations	None	None
SC. DontODPatient	Environment damages hardware	A cosmic ray flips a bit in the pump, making it run	None	Testing: Subject the pump to various environmental problems	Preemptive: Self-test	Compensation: ECC Memory	Isolation: Shielding
		The pump is poorly protected from the environment and fails open due to, eg, liquids			Preemptive: Periodic pump examinations	None	Isolation: Adequate sealing, N/A: careful use in the clinical environment
SC. DontODPatient	Operator HW Mistake	The operator accidentally presses a button she didn't mean to, giving either too much drug, too strong of a drug, or drug too quickly	None	Testing: Perform user studies on the interface	None	None	Diagnosis: Thoughtful UI (re)design
SC. DontODPatient	Operator HW Wrong Choice	The operator misunderstands the patient state and / or clinical process, giving either too much drug, too strong of a drug, or drug too quickly	None	Testing: Perform user studies on the interface	None	None	Diagnosis: Thoughtful UI (re)design, periodic retraining
SC. DontODPatient	Operator SW Mistake	The operator accidentally presses a button she didn't mean to, giving either too much drug, too strong of a drug, or drug too quickly	None	Testing: Perform user studies on the interface	None	None	Diagnosis: Thoughtful UI (re)design
SC. DontODPatient	Operator SW Wrong Choice	The operator misunderstands the patient state and / or clinical process, giving either too much drug, too strong of a drug, or drug too quickly	None	Testing: Perform user studies on the interface	None	None	Diagnosis: Thoughtful UI (re)design, periodic retraining

Activity 0: Fundamentals

Step 0.2

Element:	**Successor Link Name:**	**Predecessor Link Name(s)**	**Classification**	
AppToPumpCmds	AppLogicCommands -> PCA Pump	App Logic -> AppLogicCommands	**Architectural:**	Controller -> Actuator

Activity 1: Unsafe Interactions

Step 1.1	**Step 1.2**						
	Manifestations						
Successor Dangers	**Pred. Link**	**Content**		**Halted**	**Erratic**	**Timing**	
		High	Low			Early	Late
PCAPump.TicketTooLong	App Logic -> AppLogicCommands	AppToPumpCmds.TicketTooLong	Not Hazardous	Not Hazardous	AppToPumpCmds.ErraticTicket	AppToPumpCmds.EarlyTicket	AppToPumpCmds.LateTicket
PCAPump.ErraticTicket							
PCAPump.EarlyTicket							
PCAPump.LateTicket							

Step 1.3

Externally Caused Dangers					**Proposed Mitigations**		
Successor Danger	Name	Global Env. State	Interpretation	Co-occurring Dangers	Run-time Detection	Run-time Handling	Design-time Mitigation
PCAPump. TicketTooLong	AppToPumpCmds. TicketTooLong	Patient. NearHarm	The ticket has a time value that is too long	None	None	N / A	N / A
PCAPump. ErraticTicket	AppToPumpCmds.ErraticTicket	Patient. NearHarm	The app->pump connection gets a ticket "out of the blue"	None	None	N / A	N / A
PCAPump. EarlyTicket	AppToPumpCmds.EarlyTicket	Patient. NearHarm	The app->pump connection gets a ticket "too soon" -- before it has finished handling the previous ticket	None	Concurrent: Timeouts	Rollforward: Network disables connection (and notifies the clinician?)	N / A
PCAPump. LateTicket	AppToPumpCmds.LateTicket	Patient. NearHarm	The app->pump gets a ticket late, so it's valid past the time window it should be	None	None	N / A	Timestamped tickets or tickets have a valid end-time (and the app needs a global clock)

Activity 2: Internal Faults

Step 2.1

Faults Not Considered

Guideword	Justification
Software Bug	We're using a "proven in use" network
Bad Software Design	
Compromised Software	
Compromised Hardware	
Bad Software Design	
Bad Hardware Design	
Production Defect	
Deterioration	Deterioration is not a significant source of concern over the life of the networking materials
Environment damages hardware	The app isn't responsible for network maintenance
Operator HW Mistake	The network doesn't interact directly with a human operator
Operator HW Error	
Hacked Hardware	The hospital has physical security measures in place
Hacked Software	
Operator SW Mistake	The network doesn't interact directly with a human operator
Operator SW Wrong Choice	

Step 2.2

Internally Caused Dangers

Successor Danger	Guideword	Interpretation	Co-occurring Dangers	Design-time Detection	Run-time Detection	Run-time Error Handling	Run-time Fault Handling
PCAPump. TicketTooLong	Syntax Mismatch	A ticket is issued by the app in a different format than expected by the pump, so it runs for an unintended length of time	None	Model Checking: Verify syntax of sender and receiver	None	None	None
PCAPump. EarlyTicket	Rate Mismatch	Tickets are sent from the app too quickly for the pump to handle	None	Model Checking: Verify QoS of sender and receiver	Concurrent: Timeouts	Rollforward: Network disables connection (and notifies the clinician?)	None
PCAPump. LateTicket	Rate Mismatch	The app doesn't send tickets fast enough because it thinks the pump can't handle them	None	Model Checking: Verify QoS of sender and receiver	Concurrent: Expected arrival time	Rollforward: Network disables connection (and notifies the clinician?)	None
PCAPump. TicketTooLong	Semantic Mismatch	A ticket is issued by the app in a different format than expected by the pump, so it runs for an unintended length of time	None	Testing: Verify semantics of sender and receiver	Concurrent: Messages should use some sort of semantic tag, eg, 11073 nomenclature	Rollforward: Mismatched tags mean the app switches to a safe state and notifies the clinician	None

Activity 0: Fundamentals

Element:	Successor Link Name:	Predecessor Link Name(s)	Classification	
App Logic	App Logic -> AppLogicCommands	SpO2ToApp -> App Logic	**Architectural:**	Controller
		EtCO2ToApp -> App Logic		
		RRToApp -> App Logic		

Activity 1: Unsafe Interactions

Step 1.1	Step 1.2						
	Manifestations						
Successor Dangers	**Pred. Link**	**Content**		**Halted**	**Erratic**	**Timing**	
		High	Low			Early	Late
AppToPumpCmds. TicketTooLong	SpO2ToApp -> App Logic	AppLogic. SpO2TooHigh	Not Hazardous	AppLogic. NoSpO2	Not Hazardous	AppLogic. SpO2Early	AppLogic. SpO2Late
AppToPumpCmds.ErraticTicket	EtCO2ToApp -> App Logic	Not Hazardous	AppLogic. EtCO2TooLow	AppLogic. NoEtCO2	Not Hazardous	AppLogic. EtCO2Early	AppLogic. EtCO2Late
AppToPumpCmds.EarlyTicket	RRToApp -> App Logic	AppLogic. RRTooHigh	Not Hazardous	AppLogic.NoRR	Not Hazardous	AppLogic. RREarly	AppLogic. RRLate
AppToPumpCmds.LateTicket							

Process Variable	Process Values						Unit
Patient Status	Very healthy	Quite healthy	Pretty healthy	...	A little healthy	Risk	Overdosed	N / A

Step 1.3

Externally Caused Dangers					Proposed Mitigations		
Successor Danger	Name	Ctrld Process State	Process Var. Name and Value	Interpretation	Co-occurring Dangers	Run-time Detection	Run-time Handling
AppToPumpCmds. TicketTooLong	AppLogic. SpO2TooHigh	Patient. NearHarm	Patient Status >= Risk	The feedback from all three sensors is simultaneously incorrect leading the app to believe the patient is healthy	AppLogic. EtCO2TooLow AND AppLogic. RRTooHigh	None	N / A
None	AppLogic. SpO2TooHigh	N / A	Any	The feedback from either one or two of the sensors are incorrect, but due to redundancy harm is avoided	AppLogic. EtCO2TooLow OR AppLogic. RRTooHigh OR None	Concurrent: Assume best-case reading is valid	Compensation: Require healthy reading from all three sensors
AppToPumpCmds. TicketTooLong	AppLogic. EtCO2TooLow	Patient. NearHarm	Patient Status >= Risk	The feedback from all three sensors is simultaneously incorrect	AppLogic. SpO2TooHigh AND AppLogic. RRTooHigh	None	N / A
None	AppLogic. EtCO2TooLow	N / A	Any	The feedback from either one or two of the sensors are incorrect, but due to redundancy harm is avoided	AppLogic. SpO2TooHigh OR AppLogic. RRTooHigh OR None	Concurrent: Assume best-case reading is valid	Compensation: Require healthy reading from all three sensors
AppToPumpCmds. TicketTooLong	AppLogic. RRTooHigh	Patient. NearHarm	Patient Status >= Risk	The feedback from all three sensors is simultaneously incorrect	AppLogic. SpO2TooHigh AND AppLogic. EtCO2TooLow	None	N / A
None	AppLogic. RRTooHigh	N / A	Any	The feedback from either one or two of the sensors are incorrect, but due to redundancy harm is avoided	AppLogic. SpO2TooHigh OR AppLogic. EtCO2TooLow OR None	Concurrent: Assume best-case reading is valid	Compensation: Require healthy reading from all three sensors
None	AppLogic. NoSpO2	N / A	Any	The feedback from a sensor is missing, but the app is built to not issue tickets if any information is missing	Any	Concurrent: Require signal from all three sensors	Rollforward: Issue zero-length ticket
None	AppLogic. NoEtCO2	N / A	Any	The feedback from a sensor is missing, but the app is built to not issue tickets if any information is missing	Any	Concurrent: Require signal from all three sensors	Rollforward: Issue zero-length ticket
None	AppLogic.NoRR	N / A	Any	The feedback from a sensor is missing, but the app is built to not issue tickets if any information is missing	Any	Concurrent: Require signal from all three sensors	Rollforward: Issue zero-length ticket
AppToPumpCmds.LateTicket	AppLogic. SpO2Early	N / A	Any	The app's ticket is late because it is handling an (or a number of) unexpected SpO2 message(s)	Any	Concurrent: Timeouts	Compensation: Drop messages violating QoS settings

AppToPumpCmds.LateTicket	AppLogic. EtCO2Early	N / A	Any	The app's ticket is late because it is handling an (or a number of) unexpected EtCO2 message(s)	Any	Concurrent: Timeouts	Compensation: Drop messages violating QoS settings
AppToPumpCmds.LateTicket	AppLogic. RREarly	N / A	Any	The app's ticket is late because it is handling an (or a number of) unexpected RR message(s)	Any	Concurrent: Timeouts	Compensation: Drop messages violating QoS settings
None	AppLogic. SpO2Late	N / A	Any	The feedback from a sensor is delayed, but the app is built to not issue tickets if any information is missing	Any	Concurrent: Require signal from all three sensors	Rollforward: Issue zero-length ticket
None	AppLogic. EtCO2Late	N / A	Any	The feedback from a sensor is delayed, but the app is built to not issue tickets if any information is missing	Any	Concurrent: Require signal from all three sensors	Rollforward: Issue zero-length ticket
None	AppLogic. RRLate	N / A	Any	The feedback from a sensor is delayed, but the app is built to not issue tickets if any information is missing	Any	Concurrent: Require signal from all three sensors	Rollforward: Issue zero-length ticket

Activity 2: Internal Faults

Step 2.1

Faults Not Considered

Guideword	Justification
Syntax Mismatch	Element is a component, not a connection
Rate Mismatch	
Semantic Mismatch	
Compromised Hardware	We're using a previously-certified MAP implementation (ie, safety assessment of the MAP itself is not part of the safety assessment of the app)
Hardware Bug	
Bad Hardware Design	
Production Defect	
Deterioration	We're using an externally maintained MAP (ie, the protection of the MAP itself is not part of the safety assessment of the app)
Environment Damages Hardware	
Adversary Accesses Hardware	
Adversary Accesses Software	
Operator HW Mistake	The app logic doesn't interact with an operator.
Operator HW Wrong Choice	
Operator SW Mistake	
Operator SW Wrong Choice	

Step 2.2

Internally Caused Dangers

Successor Danger	Guideword	Interpretation	Co-occurring Dangers	Design-time Detection	Run-time Detection	Run-time Error Handling	Run-time Fault Handling
AppToPumpCmds. TicketTooLong	Software Bug	A software bug leads to incorrect ticket calculations	None	Theorem proving: formally verify the behavior of the app logic.	None	None	None
AppToPumpCmds.ErraticTicket		A software bug leads to the app issuing tickets erratically					
AppToPumpCmds.EarlyTicket		A software bug leads to the app sending tickets earlier than it should					
AppToPumpCmds.LateTicket		A software bug leads to the app issuing tickets later than it should					
AppToPumpCmds. TicketTooLong	Bad Software Design	The app is designed for someone with a normal opioid tolerance (95% of the population) but the patient is an outlier	None	Testing and statistically-backed, "bootstrapping" certification	Concurrent: Physiological monitors	Rollforward: Use an adaptive algorithm and start with a very small dose	None
AppToPumpCmds. TicketTooLong		Other poor desgin choice leads to inappropriate-length or erratic	None			None	None
AppToPumpCmds.ErraticTicket							

AppToPumpCmds.EarlyTicket		tickets					
AppToPumpCmds.LateTicket							
AppToPumpCmds. TicketTooLong	Compromised Software	An adversary gets access to the app while it's being developed	None	None	Concurrent: Some sort of TPM-like device on the MAP itself and a cryptographic chain-of-trust	None	Isolation: Chain-of-trust violations block app launch
AppToPumpCmds.ErraticTicket							
AppToPumpCmds.EarlyTicket							
AppToPumpCmds.LateTicket							

Activity 0: Fundamentals

Element:	Successor Link Name:	Predecessor Link Name(s)	Classification	
SpO2ToApp	SpO2ToApp -> App Logic	PulseOx -> SpO2ToApp	**Architectural:**	Sensor -> Controller

Activity 1: Unsafe Interactions

Step 1.1	Step 1.2						
	Manifestations						
Successor Dangers	Pred. Link	Content		Halted	Erratic	Timing	
		High	Low			Early	Late
AppLogic.SpO2TooHigh	PulseOx -> SpO2ToApp	SpO2ToApp. SpO2TooHigh	Not Hazardous	SpO2ToApp. NoSpO2	Not Hazardous	SpO2ToApp. SpO2Early	SpO2ToApp. SpO2Late
AppLogic.NoSpO2							
AppLogic.SpO2Early							
AppLogic.SpO2Late							

Step 1.3

Externally Caused Dangers					Proposed Mitigations		
Successor Danger	Name	Ctrld Process State	Process Var. Name and Value	Interpretation	Co-occurring Dangers	Run-time Detection	Run-time Handling
AppLogic. SpO2TooHigh	SpO2ToApp. SpO2TooHigh	Patient. NearHarm	Patient SpO2 > Actual Value	The feedback from the SpO2 sensor is higher than its actual value	None	None	None
AppLogic. NoSpO2	SpO2ToApp. NoSpO2	Any	None	There is no feedback from the SpO2 sensor	None	None	None
AppLogic. SpO2Early	SpO2ToApp. SpO2Early	Any	Any	The feedback from the SpO2 sensor arrives earlier than it should	None	Concurrent: Timeouts	Rollforward: Network disables connection (and notifies the clinician?)
AppLogic. SpO2Late	SpO2ToApp. SpO2Late	Any	Any	The feedback from the SpO2 sensor arrives later than it should	None	None	None

Activity 2: Internal Faults

Step 2.1

Faults Not Considered

Guideword	Justification
Software Bug	We're using a "proven in use" network
Bad Software Design	
Compromised Software	
Compromised Hardware	
Bad Software Design	
Bad Hardware Design	
Production Defect	
Deterioration	Deterioration is not a significant source of concern over the life of the networking materials
Environment damages hardware	The app isn't responsible for network maintenance
Operator HW Mistake	The network doesn't interact directly with a human operator
Operator HW Error	
Hacked Hardware	The hospital has physical security measures in place
Hacked Software	
Operator SW Mistake	The network doesn't interact directly with a human operator
Operator SW Wrong Choice	

Step 2.2

Internally Caused Dangers

Successor Danger	Guideword	Interpretation	Co-occurring Dangers	Design-time Detection	Run-time Detection	Run-time Error Handling	Run-time Fault Handling
AppLogic. SpO2TooHigh	Syntax	The SpO2 message is in a different syntactic format than what the app is expecting, so the app misinterprets it, leading to the app reading an inflated SpO2 value	None	Model Checking or Testing: Verify that syntax of SpO2	None	N / A	None

AppLogic. NoSpO2	Mismatch	The SpO2 message is in a different syntactic format than what the app is expecting, so the app can't understand it, leading to the app having no SpO2 value	None	value used by Pulse Oximeter matches that used by app	None	N / A	None
AppLogic. SpO2TooHigh	Semantic Mismatch	The underlying meaning of the SpO2 value produced by the puse oximeter isn't the same as the underlying meaning assigned to the value by the app, leading to the app interpreting an inflated SpO2 value	None	N/A: Standardize semantics at ecosphere level	Concurrent: Messages should use some sort of semantic tag, eg, 11073 nomenclature	Rollforward: Mismatched tags mean the app switches to a safe state and notifies the clinician	None
AppLogic. SpO2Early	Rate Mismatch	The pulse oximeter sends SpO2 messages faster than the app is expecting / can handle them	None	Static Analysis: Verify that RT / QoS specifications cannot be violated	Concurrent: Specified RT / QoS Properties	If messages arrive faster than allowed the network drops them and the app switches into a safe state	None
AppLogic. SpO2Late		The pulse oximeter doesn't send SpO2 messages as frequently as the app needs them				If messages don't arrive as frequently as specified the app switches into a safe state and notifies the clinician	

Activity 0: Fundamentals

Step 0.2

Element:	**Successor Link Name:**	**Predecessor Link Name(s)**	**Classification**	
Pulse Ox	PulseOx -> SpO2ToApp	PatientToPulseOx -> PulseOx	**Architectural:**	Sensor

Activity 1: Unsafe Interactions

Step 1.1	**Step 1.2**						
	Manifestations						
Successor Dangers	**Pred. Link**	**Content**		**Halted**	**Erratic**	**Timing**	
		High	Low			Early	Late
SpO2ToApp.SpO2TooHigh	PatientToPulseOx -> PulseOx	PulseOx. HighReading	Not Hazardous	PulseOx. NoConnection	Not Hazardous	PulseOx. EarlyReading	PulseOx. LateReading
SpO2ToApp.NoSpO2							
SpO2ToApp.SpO2Early							
SpO2ToApp.SpO2Late							

Process Variable	**Process Values**							**Unit**
Patient SpO2	100%	99%	98%	...	2%	1%	0%	Percentage

Step 1.3

Externally Caused Dangers					**Proposed Mitigations**		
Successor Danger	Name	Ctrld Process State	Process Var. Name and Value	Interpretation	Co-occurring Dangers	Run-time Detection	Run-time Handling
SpO2ToApp. SpO2TooHigh	PulseOx. HighReading	Patient.Near Harm	Patient SpO2 > Read value	The pulse oximeter gets a bad reading from its patient-attachment (eg, finger clip)	None	Concurrent: Use a sensor with a data-quality reading	Rollforward: Drop readings without adequate quality (transforming this into NoSpO2)
SpO2ToApp. NoSpO2	PulseOx. NoConnection	Any	Any	The pulse oximeter's patient-attachment becomes disconnected or otherwise stops producing data	None	None	N / A
None	PulseOx. EarlyReading	Any	Any	The pulse oximeter's patient-attachment produces messages faster than the pulse-oximeter itself expects them	None	Concurrent: RT / QoS specifications	Rollforward: Drop readings that arrive too early
None	PulseOx. LateReading	Any	Any	The pulse oximeter's patient-attachment produces messages slower than the pulse-oximeter itself expects them	None	Concurrent: RT / QoS specifications	Rollforward: Notify clinician and stop producing data (transforming this into NoSpO2)

Activity 2: Internal Faults

Step 2.1

Faults Not Considered

Guideword	Justification
Software Bug	We're using a "proven in use" pulse oximeter
Bad Software Design	
Compromised Software	
Compromised Hardware	
Hardware Bug	
Bad Hardware Design	
Production Defect	
Adversary Accesses Hardware	The hospital has physical security measures in place
Adversary Accesses Software	
Operator HW Mistake	There are no user settings used for the pulse oximeter
Operator HW Wrong Choice	

Operator SW Mistake	There are no user settings used for the pulse oximeter
Operator SW Mistake	
Syntax Mismatch	The pulse oximeter isn't a connection between two components
Rate Mismatch	
Semantic Mismatch	

Step 2.2

Internally Caused Dangers

Successor Danger	Guideword	Interpretation	Co-occurring Dangers	Design-time Detection	Run-time Detection	Run-time Error Handling	Run-time Fault Handling
SpO2ToApp. SpO2TooHigh	Environment damages hardware	A cosmic ray flips a bit in the PulseOx, breaking it in any possible way	None	None	Preemptive: Self-test	Compensation: ECC Memory	Isolation: Shielding
SpO2ToApp. SpO2TooHigh		The pulse oximeter is poorly protected from the environment and fails due to, eg, liquids		Testing: Subject the PulseOx to various environmental problems	Preemptive: Periodic pulseox examinations	Compensation: Additional physiological monitors should be used in case of errors with the pulse oximeter	Isolation: Adequate sealing, N/A: careful use in the clinical environment
SpO2ToApp. NoSpO2							
SpO2ToApp. SpO2Early							
SpO2ToApp. SpO2Late							
SpO2ToApp. NoSpO2	Deterioration	The pulse oximeter is poorly maintained and fails due to deterioration	None	Testing: Maintenance intervals should be established by the manufacturer and verified by regulators	Preemptive: Periodic examinations	None	None

Activity 0: Fundamentals

Element:	Successor Link Name:	Predecessor Link Name(s)	Classification	
EtCO2ToApp	EtCO2ToApp -> App Logic	Capnograph -> EtCO2ToApp	**Architectural:**	Sensor -> Controller

Activity 1: Unsafe Interactions

Step 1.1	Step 1.2						
	Manifestations						
Successor Dangers	Pred. Link	Content		Halted	Erratic	Timing	
		High	Low			Early	Late
AppLogic.EtCO2TooLow	Capnograph -> EtCO2ToApp	Not Hazardous	EtCO2ToApp. EtCO2TooLow	EtCO2ToApp. NoEtCO2	Not Hazardous	EtCO2ToApp. EtCO2Early	EtCO2ToApp. EtCO2Late
AppLogic.NoEtCO2							
AppLogic.EtCO2Early							
AppLogic.EtCO2Late							

Step 1.3

Externally Caused Dangers					Proposed Mitigations		
Successor Danger	Name	Ctrld Process State	Process Var. Name and Value	Interpretation	Co-occurring Dangers	Run-time Detection	Run-time Handling
AppLogic. EtCO2TooLow	EtCO2ToApp. EtCO2TooLow	Patient. NearHarm	Patient EtCO2 < Actual Value	The feedback from the EtCO2 sensor is lower than its actual value	None	None	None
AppLogic. NoEtCO2	EtCO2ToApp. NoEtCO2	Any	Any	There is no feedback from the EtCO2 sensor	None	None	None
AppLogic. EtCO2Early	EtCO2ToApp. EtCO2Early	Any	Any	The feedback from the EtCO2 sensor arrives earlier than it should	None	Concurrent: Timeouts	Rollforward: Network disables connection (and notifies the clinician?)
AppLogic. EtCO2Late	EtCO2ToApp. EtCO2Late	Any	Any	The feedback from the EtCO2 sensor arrives later than it should	None	None	None

Activity 2: Internal Faults

Step 2.1

Faults Not Considered

Guideword	Justification
Software Bug	We're using a "proven in use" network
Bad Software Design	
Compromised Software	
Compromised Hardware	
Bad Software Design	
Bad Hardware Design	
Production Defect	
Deterioration	Deterioration is not a significant source of concern over the life of the networking materials
Environment damages hardware	The app isn't responsible for network maintenance
Operator HW Mistake	The network doesn't interact directly with a human operator
Operator HW Error	
Hacked Hardware	The hospital has physical security measures in place
Hacked Software	
Operator SW Mistake	The network doesn't interact directly with a human operator
Operator SW Wrong Choice	

Step 2.2

Internally Caused Dangers

Successor Danger	Guideword	Interpretation	Co-occurring Dangers	Design-time Detection	Run-time Detection	Run-time Error Handling	Run-time Fault Handling
AppLogic. EtCO2TooLow	Syntax	The EtCO2 message is in a different syntactic format than what the app is expecting, so the app misinterprets it, leading to the app reading a deflated EtCO2 value	None	Model Checking or Testing: Verify that syntax of EtCO2 values	None	N / A	None

AppLogic. NoEtCO2	Mismatch	The EtCO2 message is in a different syntactic format than what the app is expecting, so the app can't understand it, leading to the app having no EtCO2 value	None	EtCO2 values used by Capnograph matches that used by app	None	N / A	None
AppLogic. EtCO2TooLow	Semantic Mismatch	The underlying meaning of the EtCO2 value produced by the puse oximeter isn't the same as the underlying meaning assigned to the value by the app, leading to the app interpreting a deflated EtCO2 value	None	N/A: Standardize semantics at ecosphere level	Concurrent: Messages should use some sort of semantic tag, eg, 11073 nomenclature	Rollforward: Mismatched tags mean the app switches to a safe state and notifies the clinician	None
AppLogic. EtCO2Early	Rate Mismatch	The pulse oximeter sends EtCO2 messages faster than the app is expecting / can handle them	None	Static Analysis: Verify that RT / QoS specifications cannot be violated	Concurrent: Specified RT / QoS Properties	If messages arrive faster than allowed the network drops them and the app switches into a safe state	None
AppLogic. EtCO2Late		The pulse oximeter doesn't send EtCO2 messages as frequently as the app needs them				If messages don't arrive as frequently as specified the app switches into a safe state and notifies the clinician	

Activity 0: Fundamentals

Element:	Successor Link Name:	Predecessor Link Name(s)	Classification	
RRToApp	RRToApp -> App Logic	PulseOx -> RRToApp	**Architectural:**	Sensor -> Controller

Activity 1: Unsafe Interactions

Step 1.1	Step 1.2						
	Manifestations						
Successor Dangers	**Pred. Link**	**Content**		**Halted**	**Erratic**	**Timing**	
		High	Low			Early	Late
AppLogic.RRTooHigh	PulseOx -> RRToApp	RRToApp. RRTooHigh	Not Hazardous	RRToApp. NoRR	Not Hazardous	RRToApp. RREarly	RRToApp. RRLate
AppLogic.NoRR							
AppLogic.RREarly							
AppLogic.RRLate							

Step 1.3

Externally Caused Dangers					Proposed Mitigations		
Successor Danger	Name	Ctrld Process State	Process Var. Name and Value	Interpretation	Co-occurring Dangers	Run-time Detection	Run-time Handling
AppLogic. RRTooHigh	RRToApp. RRTooHigh	Patient. NearHarm	Patient RR > Actual Value	The feedback from the RR sensor is higher than its actual value	None	None	None
AppLogic.NoRR	RRToApp. NoRR	Any	Any	There is no feedback from the RR sensor	None	None	None
AppLogic. RREarly	RRToApp. RREarly	Any	Any	The feedback from the RR sensor arrives earlier than it should	None	Concurrent: Timeouts	Rollforward: Network disables connection (and notifies the clinician?)
AppLogic. RRLate	RRToApp. RRLate	Any	Any	The feedback from the RR sensor arrives later than it should	None	None	None

Activity 2: Internal Faults

Step 2.1

Faults Not Considered

Guideword	Justification
Software Bug	We're using a "proven in use" network
Bad Software Design	
Compromised Software	
Compromised Hardware	
Bad Software Design	
Bad Hardware Design	
Production Defect	
Deterioration	Deterioration is not a significant source of concern over the life of the networking materials
Environment damages hardware	The app isn't responsible for network maintenance
Operator HW Mistake	The network doesn't interact directly with a human operator
Operator HW Error	
Hacked Hardware	The hospital has physical security measures in place
Hacked Software	
Operator SW Mistake	The network doesn't interact directly with a human operator
Operator SW Wrong Choice	

Step 2.2

Internally Caused Dangers

Successor Danger	Guideword	Interpretation	Co-occurring Dangers	Design-time Detection	Run-time Detection	Run-time Error Handling	Run-time Fault Handling
AppLogic. RRTooHigh	Syntax	The RR message is in a different syntactic format than what the app is expecting, so the app misinterprets it, leading to the app reading an inflated RR value	None	Model Checking or Testing: Verify that syntax of RR	None	N / A	None

AppLogic.NoRR	Mismatch	The RR message is in a different syntactic format than what the app is expecting, so the app can't understand it, leading to the app having no RR value	None	values used by Capnograph matches that used by app	None	N / A	None
AppLogic. RRTooHigh	Semantic Mismatch	The underlying meaning of the RR value produced by the puse oximeter isn't the same as the underlying meaning assigned to the value by the app, leading to the app interpreting an inflated RR value	None	N/A: Standardize semantics at ecosphere level	Concurrent: Messages should use some sort of semantic tag, eg, 11073 nomenclature	Rollforward: Mismatched tags mean the app switches to a safe state and notifies the clinician	None
AppLogic. RREarly	Rate Mismatch	The pulse oximeter sends RR messages faster than the app is expecting / can handle them	None	Static Analysis: Verify that RT / QoS specifications cannot be violated	Concurrent: Specified RT / QoS Properties	If messages arrive faster than allowed the network drops them and the app switches into a safe state	None
AppLogic. RRLate		The pulse oximeter doesn't send RR messages as frequently as the app needs them				If messages don't arrive as frequently as specified the app switches into a safe state and notifies the clinician	

Activity 0: Fundamentals

Step 0.2

Element:	Successor Link Name(s):	Predecessor Link Name(s)	Classification	
Capnograph	Capnograph -> EtCOToApp	PatientToCapnograph -> Capnograph	**Architectural:**	Sensor
	Capnograph -> RRToApp			

Activity 1: Unsafe Interactions

Step 1.1	Step 1.2					
	Manifestations					
Successor Dangers	Pred. Link	Content	Halted	Erratic	Timing	
					Early	Late
EtCO2ToApp.EtCO2TooLow	PatientToCapnograph -> Capnograph	PatientToCapnograph.BadReading	PatientToCapnograph.NoData	Not Hazardous	PatientToCapnograph.EarlyData	PatientToCapnograph.LateData
EtCO2ToApp.NoEtCO2						
EtCO2ToApp.EtCO2Early						
EtCO2ToApp.EtCO2Late						
RRToApp.RRTooHigh						
RRToApp.NoRR						
RRToApp.RREarly						
RRToApp.RRLate						

Process Variable	Process Values							Unit
Patient EtCO2	100%	99%	98%	...	3%	2%	1%	Percent
Patient RR	75	74	73	...	2	1	0	Breaths per Minute

Step 1.3

Externally Caused Dangers					Proposed Mitigations		
Successor Danger	Name	Ctrld Process State	Process Var. Name and Value	Interpretation	Co-occurring Dangers	Run-time Detection	Run-time Handling
EtCO2ToApp. EtCO2TooLow	PatientToCapnograph. BadReading	Patient. NearHarm	EtCO2 < Actual Value	The sensor itself malfunctions, providing an over-optimistic reading of the patient's health	None	None	N / A
RRToApp. RRTooHigh			RR > Actual Value				
EtCO2ToApp. NoEtCO2	PatientToCapnograph.NoData	Any	None	The sensor stops providing any information at all, so the capnograph also can't produce any output	None	None	N / A
RRToApp. NoRR							
None	PatientToCapnograph.EarlyData	Any	Any	The capnograph's patient-attachment produces messages faster than the capnograph itself expects them	None	Concurrent: RT / QoS specifications	Rollforward: Drop readings that arrive too early
None	PatientToCapnograph.LateData	Any	Any	The capnograph's patient-attachment produces messages slower than the capnograph itself need them	None	Concurrent: RT / QoS specifications	Rollforward: Notify clinician and stop producing data (transforming this into NoSpO2)

Activity 2: Internal Faults

Step 2.1

Faults Not Considered

Guideword	Justification
Software Bug	We're using a "proven in use" capnograph
Bad Software Design	
Compromised Software	
Compromised Hardware	
Hardware Bug	
Bad Hardware Design	

Production Defect	
Adversary Accesses Hardware	The hospital has physical security measures in place
Adversary Accesses Software	
Operator HW Mistake	There are no user settings used for the capnograph
Operator HW Wrong Choice	
Operator SW Mistake	
Operator SW Mistake	
Syntax Mismatch	The capnograph isn't a connection between two components
Rate Mismatch	
Semantic Mismatch	

Step 2.2

Internally Caused Dangers

Successor Danger	Guideword	Interpretation	Co-occurring Dangers	Design-time Detection	Run-time Detection	Run-time Error Handling	Run-time Fault Handling
EtCO2ToApp. EtCO2TooLow	Environment damages hardware	A cosmic ray flips a bit in the Capnograph, breaking it in any possible way	None	None	Preemptive: Self-test	Compensation: ECC Memory	Isolation: Shielding
RRToApp. RRTooHigh							
EtCO2ToApp. EtCO2TooLow		The capnograph is poorly protected from the environment and fails due to, eg, liquids		Testing: Subject the capnograph to various environmental problems	Preemptive: Periodic pump examinations	Compensation: Additional physiological monitors should be used in case of errors with the pulse oximeter	Isolation: Adequate sealing, N/A: careful use in the clinical environment
EtCO2ToApp. NoEtCO2							
EtCO2ToApp. EtCO2Early							
EtCO2ToApp. EtCO2Late							
RRToApp. RRTooHigh							
RRToApp. NoRR							
RRToApp. RREarly							
RRToApp. RRLate							
EtCO2ToApp. NoEtCO2	Deterioration	The capnograph is poorly maintained and fails due to deterioration	None	Maintenance intervals should be established by the manufacturer and verified by	Preemptive: Routine Maintenance	None	None
RRToApp. NoRR							

	A	B	C	D	E	F	G	H	I	J	K
1	**System:**	PCA Interlock								**System Boundary**	
2		**Fundamentals**								System	Environment
3		Name	Reference							PCA Pump	Patient
4										App Logic	
5	Accident Levels:	AL. DeathOrSeriousInjury	N / A							Pulse Oximeter	
6										Capnograph	
7	Accidents:	Acc. PatientHarmed	AL. DeathOrSeriousInjury								
8				Hazardous Factor	System Element	System Element State	Env. Element	Env. Element State			
9	Hazards:	H. TooMuchAnalgesic	Acc. PatientHarmed	Analgesic	PCA Pump	Pumping	Patient	NearHarm			
10											
11	Safety Constraints:	SC. DontODPatient	H. TooMuchAnalgesic								
12											
13	**Explanations**										
14	Reference	Explanation									
15	Acc. PatientHarmed	The patient is harmed or seriously injured as a result of the App's actions or inaction									
16	H. TooMuchAnalgesic	The patient is given more analgesic than he / she can safely tolerate									
17	Architecture	As modeled by Arney-etal in ICCPS10 (in section 4.3) with some modifications									
18		A lot of possibly unmeetable assumptions (guaranteed timing of network and app)									
19		Modified to include RR and EtCO2 physiological monitors (in addition to SpO2)									

	A	B	C	D	E	F	G	H	I
1	**Activity 0: Fundamentals**								
2	**Step 0.2**								
3	**Element:**		**Successor Link Name:**		**Predecessor Link Name(s)**		**Classification**		
4	PCA Pump		PCA Pump -> IV Line		AppLogicCommands -> PCA Pump		**Architectural:**	Actuator	
5									
6	**Activity 1: Unsafe Interactions**								
7	**Step 1.1**		**Step 1.2**						
8			**Manifestations**						
9	**Successor Dangers**		**Pred. Link**	**Content**		**Halted**	**Erratic**	**Timing**	
10				High	Low			Early	Late
11	SC.DontODPatient		AppLogicCommands -> PCA Pump	PCAPump. TicketTooLong	Not Hazardous	Not Hazardous	PCAPump. ErraticTicket	PCAPump. EarlyTicket	PCAPump. LateTicket
12									
13	**Process Variable**	**Process Values**							**Unit**
14	Ticket Duration	1	2	3	...	598	599	600	Seconds
15									
16	**Step 1.3**								
17	**Externally Caused Dangers**							**Proposed Mitigations**	
18	Successor Danger	Name	Process Var. Name	Process Var. Value	Interpretation		Co-occurring Dangers	Run-time Detection	Run-time Handling
19	SC. DontODPatient	PCAPump. TicketTooLong	Ticket Duration	Higher than safe	The PCA pump receives a non-zero ticket when the patient cannot tolerate any more analgesic, which leads to the pump administering drug when it should not.		None	None	N / A
20	SC. DontODPatient	PCAPump. ErraticTicket	Ticket Duration	Any	*(Removed Due to Space Constraints)*		None	None	N / A
21	*(Removed Due to Space Constraints)*								
22									
23	**Activity 2: Internal Faults**								
24									
25	**Step 2.1**								
26	**Faults Not Considered**								
27	Guideword		Justification						
28	Compromised Software		We're using a "proven in use" PCA Pump						
29	Bad Hardware Design								
30	Production Defect								
31	Semantic Mismatch		The PCA pump isn't a connection between two components						
32	Adversary Accesses Hardware		The hospital has physical security measures in place						
33	*(Removed Due to Space Constraints)*								
34									
35	**Step 2.2**								
36	**Internally Caused Dangers**								
37	Successor Danger	Guideword	Interpretation		Co-occurring Dangers	Design-time Detection	Run-time Detection	Run-time Error Handling	Run-time Fault Handling
38	SC. DontODPatient	Deterioration	The pump is poorly maintained and fails open due to deterioration		None	Testing: Maintenance intervals should be estab. by the manufacturers and verified by regulators	Preemptive: Periodic pump examinations	None	None
39	SC. DontODPatient	Operator HW Wrong Choice	The operator misunderstands the patient state and / or clinical process, giving either too much drug, too strong of a drug, or drug too quickly		None	Testing: Perform user studies on the interface	None	None	Diagnosis: Thoughtful UI (re)design, periodic retraining
40	*(Removed Due to Space Constraints)*								