System:	PCA Interlock							System I	Boundary
	Funda	mentals						System	Environment
	Name	Reference						PCA Pump	Patient
								App Logic	
Accident Levels:	AL. DeathOrSerious Injury	N / A						Pulse Oximeter	
								Capnograph	
Accidents:	Acc. PatientHarmed	AL. DeathOrSerious Injury							
			Hazardous Factor	System Element	System Element State	Env. Element	Env. Element State		
Hazards:	H. TooMuchAnalg esic	Acc. PatientHarmed	Analgesic	PCA Pump	Pumping	Patient	NearHarm		
Safety Constraints:	SC. DontODPatient	H. TooMuchAnalg esic							
				Explanations	3				
Reference				Exp	lanation				
Acc. PatientHarmed	The patient is ha	rmed or seriously	injured as a resi	ult of the App's a	ctions				
H. TooMuchAnalg esic	The patient is given	ven more analges	ic than they can	safely tolerate					
Architecture	As modeled by A	Arney-etal in ICCP	S10 (in section 4	1.3) with some me	odifications				
	A lot of possibly	unmeetable assu	mptions (guarant	eed timing of net	work and app)				
	Modified to inclu	de RR and EtCO2	2 physiological m	onitors (in additio	on to SpO2)				

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

			Activit	y 0: Fundam	entals			
				Step 0.2				
Elen	nent:	Successor	Link Name:	Predecessor	Link Name(s)		Classification	
PCA Pump		PCA Pump -> IV	Line	AppLogicCommar	nds -> PCA Pump	Architectural:	Actuator	
			Activity 1	: Uncofo Int/	aractions			
01			ACTIVITY	. Unsale inte				
Step	0 1.1				Step 1.2			
•					Manifestations			
Successo	r Dangers	Pred. Link	Cor	itent	Halted	Erratic	l In	ning
		Appl ogioComm	High	LOW			Early	Late
SC.DontC	DPatient	ands -> PCA Pump	PCAPump. TicketTooLong	Not Hazardous	Not Hazardous	PCAPump. ErraticTicket	PCAPump. EarlyTicket	PCAPump. LateTicket
Process								
Variable				Process Values				Unit
Ticket Duration	1	2	3	3 598			600	Seconds
				Step 1.3				
		Exte	ernally Caused Da	ngers			Proposed	Mitigations
Successor	Namo	Process Var.	Process Var.	Interne	atation	Co-occurring	Run-time	Run-time
SC	PCAPump	Indiffe	value	Interpretation L		Dangers	Detection	Tanuling
DontODPatient	TicketTooLong	Ticket Duration	Higher than safe	The ticket has a time value that is too long		None	None	N / A
SC.	PCAPump. ErraticTicket	Ticket Duration	Anv	The PCA Pump ge	ets a ticket "out of	None	None	N / A
SC. DontODPatient	PCAPump. EarlyTicket	Ticket Duration	Any	The PCA Pump gets a ticket "too soon" before it has finished bandling the previous ticket		None	Concurrent: Timeouts	Rollforward: Pump switches into permanent KVO (and notifies the clinician?)
SC.	PCAPump.	Ticket Duration	Anv	The PCA pump g so it's valid past th	ets a ticket late, ne time window it	None	Concurrent: Timestamped	Rollforward: Pump switches
DOILODFallent	Latericket			Shou		None	lickels	
		1	Activit	y 2: Internal	Faults			
				Step 2.1				
			Fa	uits Not Considere	ea			
Guide	eword				Justification			
Sollware Bug	oian							
Compromised Se	sign							
Compromised St	ontware	We're using a "p	oven in use" PCA	Pump				
Hordworo Bug	aluwale	were using a p		lump				
Bad Hardware D	esian							
Production Defer	*							
Adversary Acces	ses Hardware							
Adversary Acces	ses Software	The hospital has	physical security n	neasures in place				
Syntax Miematch								
Rate Mismatch	<u> </u>	The PCA nump i	sn't a connection b	etween two compor	nents			
Semantic Misma	tch							
				Step 2.2				1
			Inter	nally Caused Dan	gers			
Successor				Co-occurring	Design-time	Run-time	Run-time	Run-time
Danger	Guideword	Interp	retation	Dangers	Detection	Detection	Error Handling	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
		A cosmic ray flips a bit in the pump, making it run		Testing: Subject	Preemptive: Self-test	Compensation: ECC Memory	Isolation: Shielding
SC. DontODPatient	Environment damages hardware	The pump is poorly protected from the environment and fails open due to, eg, liquids	None	the pump to various environmental problems	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: Fundam	nentals			
				Step 0.2				
Eler	nent:	Successor	Link Name:	Predecessor	Link Name(s)		Classification	
AppToPumpCm	ds	AppLogicComma Pump	ands -> PCA	App Logic -> AppL	ogicCommands	Architectural:	Controller	-> Actuator
			Activity 1	: Unsafe Inte	eractions			
Ste	p 1.1				Step 1.2			
					Manifestations			
Successo	or Dangers	Brod Link	Con	itent	Haltad	Errotio	Tin	ning
		Fieu. Lilik	High	Low	Halleu	Litatic	Early	Late
PCAPump.T	ïcketTooLong	App Logic -> AppLogicComm ands	AppToPumpCmd s.TicketTooLong	Not Hazardous	Not Hazardous	AppToPumpCm ds.ErraticTicket	AppToPumpCm ds.EarlyTicket	AppToPumpCm ds.LateTicket
PCAPump.	ErraticTicket							
PCAPump	.EarlyTicket							
PCAPump	.LateTicket							
				Step 1.3				
		Externally C	aused Dangers			Pr	oposed Mitigatio	ons
Successor	Namo	Global Env.	Inform	atation	Co-occurring	Run-time	Run-time	Design-time
Danger	Name	State	Interpr	etation	Dangers	Detection	Handling	witigation
PCAPump. ds. Patient. The ticket has TicketTooLong TicketTooLong NearHarm			The ticket has a t too	time value that is long	None	None	N/A	N/A
PCAPump.	AppToPumpCm	Patient.	The app->pump of	connection gets a				
ErraticTicket	ds.ErraticTicket	NearHarm	ticket "out	of the blue"	None	None	N/A	N / A
PCAPump. EarlyTicket	AppToPumpCm ds.EarlyTicket	Patient. NearHarm	The app->pump o ticket "too soon" finished handling	connection gets a ' before it has the previous ticket	None	Concurrent: Timeouts	Network disables connection (and notifies the clinician?)	N / A
PCAPump. LateTicket	AppToPumpCm ds.LateTicket	Patient. NearHarm	The app->pump ge it's valid past the shou	ets a ticket late, so e time window it Id be	None	None	N / A	Timestamped tickets or tickets have a valid end-time (and the app needs a global clock)
			Activit	v 2. Internal	Faults			
			Activit	y 2. mternar	auns			
				Step 2.1				
			Fai	ults Not Considere	ed			
Guid	eword				Justification			
Software Bug								
Bad Software De	esign							
Compromised S	oftware							
Compromised H	ardware	We're using a "p	roven in use" netwo	ork				
Bad Software De	esign							
Bad Hardware D	esign							
Production Defe	ct							
Deterioration		Deterioration is r	ot a significant sou	rce of concern over	the life of the net	working materials		
Environment dar	mages hardware	The app isn't res	ponsible for networ	k maintenance				
Operator HW Mi	perator HW Mistake							
Operator HW Er	perator HW Error							
Hacked Hardwar	lacked Hardware The hospital has physical security measures in place							
Hacked Software	e		, ,, ,, ,, ,, ,, ,					
Operator SW Mi	stake	The network doe	sn't interact directly	with a human oper	rator			
Operator SW Wr	rong Choice							
				Stop 2.2				
					nore			
			inter	nany caused Dang	9013			

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

			Activit	y 0: Fundam	nentals					
Activity 0: Fundamentals Element: Successor Link Name: Predecessor Link Name(s)						Classification				
Арр	Logic	App Logic -> Ap	pLogicCommands	SpO2ToApp	-> App Logic	Architectural:	Con	troller		
				EtCO2ToApp	-> App Logic					
				RRToApp -	> App Logic					
			Activity 1	: Unsafe Inte	eractions					
Ste	o 1.1		Step 1.2							
					Manifestations					
Successo	or Dangers	Dread Linds	Cor	ntent		Functio	Tin	ning		
		Pred. Link	High	Low	Haited	Erratic	Early	Late		
AppToPu	mpCmds.	SpO2ToApp ->	AppLogic.	Netllemendeur	AppLogic.	Natilaradaus	AppLogic.	AppLogic.		
TICKET	ooLong		SpO2100High	Not Hazardous		Not Hazardous	SpO2Early	Appl ogic		
AppToPumpCm	nds.ErraticTicket	App Logic	Not Hazardous	EtCO2TooLow NoEtCO2 N		Not Hazardous	EtCO2Early	EtCO2Late		
		RRToApp ->	AppLogic.				AppLogic.	AppLogic.		
AppToPumpCr	nds.EarlyTicket	App Logic	RRTooHigh	Not Hazardous	AppLogic.NoRR	Not Hazardous	RREarly	RRLate		
AppToPumpC	mds.Late Licket									
Brocoss										
Variable				Process Values				Unit		
Patient Status	Very healthy	Quite healthy	Pretty healthy		A little healthy	Risk	Overdosed	N / A		
				Step 1.3						
		Externally C	Caused Dangers			Pr	ons			
Successor Danger	Name	Ctrld Process State	Process Var. Name and Value	Interpr	etation	Co-occurring Dangers	Run-time Detection	Run-time Handling		
AppToPumpCm ds.	AppLogic.	Patient.	Patient Status >=	The feedback sensors is simulta leading the app	from all three neously incorrect to believe the	AppLogic. EtCO2TooLow AND AppLogic.				
TicketTooLong	SpO2TooHigh	NearHarm	Risk	patient is	s healthy	RRTooHigh	None	N / A		
None	AppLogic. SpO2TooHigh	N/A	Anv	The feedback fro two of the senso but due to redur avoi	om either one or ors are incorrect, ndancy harm is ided	AppLogic. EtCO2TooLow OR AppLogic. RRTooHigh OR None	Concurrent: Assume best- case reading is valid	Compensation: Require healthy reading from all three sensors		
AppToPumpCm ds. TicketTooLong	AppLogic. EtCO2TooLow	Patient. NearHarm	Patient Status >= Risk	The feedback sensors is simulta	from all three aneously incorrect	AppLogic. SpO2TooHigh AND AppLogic. RRTooHigh	None	N/A		
None	AppLogic. EtCO2TooLow	N/A	Any	The feedback fro two of the senso but due to redur avoi	om either one or ors are incorrect, ndancy harm is ided	AppLogic. SpO2TooHigh OR AppLogic. RRTooHigh OR None	Concurrent: Assume best- case reading is valid	Compensation: Require healthy reading from all three sensors		
AppToPumpCm ds. TicketTooLong	AppLogic. RRTooHigh	Patient. NearHarm	Patient Status >= Risk	The feedback sensors is simulta	from all three aneously incorrect	AppLogic. SpO2TooHigh AND AppLogic. EtCO2TooLow	None	N/A		
None	AppLogic. RRTooHigh	N / A	Any	The feedback fro two of the senso but due to redur avoi	om either one or ors are incorrect, ndancy harm is ided	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 fr missing, but the a issue tickets if ar miss	The feedback from a sensor is missing, but the app is built to not issue tickets if any information is		Concurrent: Require signal from all three sensors	Rollforward: Issue zero- length ticket		
None	AppLogic.NoRR	N/A	Any	The feedback fr missing, but the a issue tickets if ar miss	rom a sensor is app is built to not ny information is sing	Any	Concurrent: Require signal from all three sensors	Rollforward: Issue zero- length ticket		
AppToPumpCm ds.LateTicket	AppLogic. SpO2Early	N / A	Any	The app's ticket is handling an (or unexpected Spr	late because it is r a number of) O2 message(s)	Any	Concurrent: Timeouts	Compensation: Drop messages violating QoS settings		

AppToPumpCm ds.LateTicket	AppLogic. EtCO2Early	N / A	Any	The app's ticket is handling an (c unexpected Et(s late because it is or a number of) CO2 message(s)	Any	Concurrent: Timeouts	Compensation: Drop messages violating QoS settings				
AppToPumpCm ds.LateTicket	AppLogic. RREarly	N / A	Any	The app's ticket is handling an (c unexpected F	s late because it is or a number of) RR message(s)	Any	Concurrent: Timeouts	Compensation: Drop messages violating QoS settings				
None	AppLogic. SpO2Late	N / A	Anv	The feedback f delayed, but the issue tickets if a mis	rom a sensor is app is built to not ny information is asing	Anv	Concurrent: Require signal from all three sensors	Rollforward: Issue zero- length ticket				
None	AppLogic. EtCO2Late	N / A	Any	The feedback f delayed, but the issue tickets if a mis	rom a sensor is app is built to not ny information is ssing	Any	Concurrent: Require signal from all three sensors	Rollforward: Issue zero- length ticket				
None	AppLogic. RRLate	N / A	Any	The feedback f delayed, but the issue tickets if a mis	rom a sensor is app is built to not ny information is ssing	Any	Concurrent: Require signal from all three sensors	Rollforward: Issue zero- length ticket				
			Activit	y 2: Internal	Faults							
				Step 2.1								
			Fa	ults Not Conside	red							
Guide	eword				Justification							
Syntax N	lismatch											
Rate M	ismatch			Element is a component, not a connection								
Semantic	Mismatch											
Compromise	ed Hardware											
Hardwa	are Bug	We're using a	previously-certifie	d MAP implementa	tion (ie, safety asse	essment of the M	AP itself is not par	t of the safety				
Bad Hardw	are Design			ass	sessment of the app))						
Productio	on Defect											
Deterio	oration											
Environment Dar	mages Hardware	We're using an	externally maintai	ained MAP (ie, the protection of the MAP itself is not part of the safety assessment of the								
Adversary Acce	esses Hardware				app)							
Adversary Acce	esses Software											
Operator H	W Mistake											
Operator HW	Wrong Choice			The app logic o	loesn't interact with	an operator						
Operator S	W Mistake			The upp logic (an operator.						
Operator SW	Wrong Choice											
				Step 2.2								
			Inter	nally Caused Dar	ngers							
Successor	Guideword	Internr	retation	Co-occurring Dangers	Design-time	Run-time	Run-time Error Handling	Run-time				
AppToPumpCm	Caldoword			Langero	Deteotion	Deteotion		. dait nananny				
ds. TicketTooLong		A software bug le ticket cal	eads to incorrect lculations		Theorem							
AppToPumpCm ds.ErraticTicket	Software Bug	A software bug I issuing ticke	leads to the app ets erratically	None	proving: formally verify	None	None	None				
AppToPumpCm ds.EarlyTicket		A software bug I sending tickets sho	leads to the app s earlier than it buld		the behavior of the app logic.							
AppToPumpCm ds.LateTicket		A software bug I issuing tickets la	leads to the app ter than it should									
AppToPumpCm ds. TicketTooLong		The app is design with a normal o (95% of the pop patient is	ned for someone pioid tolerance pulation) but the an outlier	None			Rollforward: Use an adaptive algorithm and start with a very small dose	None				
AppToPumpCm ds. TicketTooLong AppToPumpCm ds.ErraticTicket	Bad Software Design	Other poor desgin inappropriate-le	n choice leads to ength or erratic	None	Testing and statistically- backed, "bootstrapping" certification	Concurrent: Physiological monitors	None	None				

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

			Activity	y 0: Fundam	entals			
Elen	nent:	Successo	r Link Name:	Predecessor I	Link Name(s)		Classification	
SpO2	ТоАрр	SpO2ToAp	p -> App Logic	PulseOx -> S	SpO2ToApp	Architectural:	Sensor ->	Controller
			Activity 1	: Unsafe Inte	eractions			
Ster	o 1.1				Step 1.2			
•					Manifestations			
Successo	or Dangers		Con	itent			Tin	ning
	•	Pred. Link	High	Low	Halted	Erratic	Early	Late
AppLogic.S	pO2TooHigh	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			Pi	oposed Mitigatic	ons
Successor		Ctrld Process	Process Var			Co-occurring	Run-time	Run-time
Danger	Name	State	Name and Value	Interpre	etation	Dangers	Detection	Handling
				The feedback f	rom the SpO2	_		
AppLogic. SpO2TooHigh	SpO2ToApp. SpO2TooHigh	Patient. NearHarm	Patient SpO2 > Actual Value	sensor is higher than its actual value		None	None	None
AppLogic.	SpO2ToApp.	A	News	There is no feedback from the		News	News	News
NoSpO2	NoSpO2	Any	None	SpO2 s	sensor	None	None	None
AppLogic. SpO2Early	SpO2ToApp. SpO2Early	Any	Any	The feedback from the SpO2 sensor arrives earlier than it should		None	Concurrent: Timeouts	Network disables connection (and notifies the clinician?)
AppLogic. SpO2Late	SpO2ToApp. SpO2Late	Any	Any	The feedback for sensor arrives late	rom the SpO2 er than it should	None	None	None
			Activity	2: Internal	Faults			
				Stop 2.4				
			Fai	ults Not Consider	he			
Guide	oword		14		luctification			
Softwara Bug	eword				Justilication			
Soliware bug								
Bad Software De	sign							
Compromised So	oftware							
Compromised Ha	ardware	We're using a "p	proven in use" netwo	ork				
Bad Software De	esign							
Bad Hardware D	esign							
Production Defe	ct							
Deterioration		Deterioration is	not a significant sou	rce of concern over	the life of the ne	tworking materials	;	
Environment dar	nages hardware	The app isn't res	sponsible for networ	k maintenance				
Operator HW Mi	stake							
Operator HW Fr	ror	The network doe	esn't interact directly	with a human ope	rator			
Hacked Hardwar	e							
Hacked Software	-	The hospital has	s physical security m	neasures in place				
Operator SM/ Mi	stako							
		The network doe	esn't interact directly	with a human ope	rator			
Operator Sw Wr	ong Choice							
				01				
				Step 2.2				
			Inter	nally Caused Dang	gers			
Successor	Quidaward	laste en	rotation	Co-occurring	Design-time	Run-time	Run-time	Run-time
AppLogic. SpO2TooHigh	Guideword	The SpO2 mess syntactic format is expectin misinterprets it,	age is in a different than what the app g, so the app leading to the app	Dangers	Model Checking or Testing: Verify that	Delection		rauit manoilng
	Syntax	reading an inf	ated SpO2 value	None	syntax of SpO2	None	Ν / Δ	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	копе	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	Pata Mismatch	The pulse oximeter sends SpO2 messages faster than the app is expecting / can handle them	Noro	Static Analysis: Verify that RT / QoS	Concurrent:	If messages arrive faster than allowed the network drops them and the app switches into a safe state	Nano
AppLogic. SpO2Late		The pulse oximeter doesn't send SpO2 messages as frequently as the app needs them	NUTE	specifications cannot be violated	QoS Properties	If messages don't arrive as frequently as specified the app switches into a safe state and notifies the clinician	None

			Activit	y 0: Fundam	entals				
				Step 0.2					
Elen	nent:	Successor	Link Name:	Predecessor I	Link Name(s)		Classification		
Puls	e Ox	PulseOx ->	SpO2ToApp	PatientToPulse	Ox -> PulseOx	Architectural:	Sei	nsor	
			Activity 1	: Unsafe Inte	eractions				
Ste	p 1.1				Step 1.2				
				I	Manifestations				
Successo	or Dangers	Brod Link	Cor	ntent	Haltod	Erratio	Tin	ning	
		Fieu. Lilik	High	Low	Haiteu	Litatic	Early	Late	
SpO2ToApp.	SpO2TooHigh	PatientToPulse Ox -> PulseOx	PulseOx. HighReading	Not Hazardous	PulseOx. NoConnection	Not Hazardous	PulseOx. EarlyReading	PulseOx. LateReading	
SpO2ToAp	p.NoSpO2								
SpO2ToApp	p.SpO2Early								
SpO2ToAp	p.SpO2Late								
Process				Process Values				Unit	
	100%	00%	0.00/	FIOCESS Values	20/	10/	0%	Dereentage	
	100 %	99%	90%		2 70	1 70	0 76	Fercentage	
				Stop 1 2					
		Extornally C	ausod Dangors	Step 1.5		Dr	onosod Mitigatic	ne	
Successor		Ctrld Process	Process Var			Co-occurring	Run-time	Run-time	
Danger	Name	State	Name and Value	Interpre	etation	Dangers	Detection	Handling	
SpO2ToApp. SpO2TooHigh	PulseOx. HighReading	Patient.Near Harm	Patient SpO2 > Read value	The pulse oxime reading from its pa (eg, fing	eter gets a bad atient-attachment ler 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 oxim attachment becom or otherwise stops	neter's patient- nes disconnected s producing data	None	None	N/A	
None	PulseOx. EarlyReading	Any	Any	The pulse oxim attachment produ faster than the puls expects	neter's patient- uces messages se-oximeter itself s them	None	Concurrent: RT / QoS specifications	Rollforward: Drop readings that arrive too early	
None	PulseOx. LateReading	Any	Any	The pulse oxim attachment produ slower than the itself expe	neter's patient- uces messages pulse-oximeter ects them	None	Concurrent: RT / QoS specifications	Rollforward: Notify clinician and stop producing data (transforming this into NoSpO2)	
			A otiviti	2. Internel	Foulto				
			ACTIVIT	y 2. mternar	rauits				
				Step 2.1					
			Fa	ults Not Considere	ed				
Guid	eword				Justification				
Software Bug									
Bad Software Design									
Compromised S	oftware								
Compromised H	ardware	We're using a "proven in use" pulse oximeter							
Hardware Bug									
Bad Hardware D	esign								
Production Defe	ct								
Adversary Acces	ses Hardware								
Adversary Acces	ses Software	The hospital has	pnysical security n	neasures in place					
Operator HW Mi	stake								
Operator HW Wr	rong Choice								

Operator SW Mistake		i nere are no us	er settings used for	the pulse oximeter	· ·						
Operator SW Mis	Operator SW Mistake										
Syntax Mismatch	ı										
Rate Mismatch		The pulse oximeter isn't a connection between two components									
Semantic Misma	tch										
				Step 2.2							
			Inter	nally Caused Dar	igers						
Successor Danger	Guideword	Inter	pretation	Co-occurring Dangers	Design-time Detection	Run-time Detection	Run-time Error Handling	Run-time Fault Handling			
SpO2ToApp. SpO2TooHigh	Environment	A cosmic ray PulseOx, bro poss	flips a bit in the eaking it in any ible way		None	Preemptive: Self-test	Compensation: ECC Memory	Isolation: Shielding			
SpO2ToApp. SpO2TooHigh SpO2ToApp.		The pulse oximeter is poorly protected from the environment	None	Testing: Subject	Preemptive:	Compensation: Additional physiological	Isolation: Adequate				
NoSpO2	hardware			the PulseOx to various Periodic r	monitors should	sealing, N/A:					
SpO2ToApp. SpO2Early		and fails du	ind fails due to, eg, liquids		environmental	pulseox examinations	be used in case of errors with	careful use in the clinical			
SpO2ToApp. SpO2Late							oximeter	environment			
SpO2ToApp. NoSpO2	Deterioration	The pulse ox maintained a dete	imeter is poorly and fails due to rioration	None	Testing: Maintenance intervals should be established by the manufacturer and verified by regulators	Preemptive: Periodic examinations	None	None			

			Activit	y 0: Fundam	entals			
Eler	nent:	Successo	r Link Name:	Predecessor	Link Name(s)		Classification	
EtCO2	2ТоАрр	EtCO2ToAp	p -> App Logic	Capnograph ->	• EtCO2ToApp	Architectural:	Sensor -> Controller	
			Activity 1	: Unsafe Inte	eractions			
Ste	n 1 1				Sten 1 2			
Ole	9 1.1				Manifestations			
Successo	r Dangore		Cor	tont	Walliestations		Tin	nina
Guttesst	Dangers	Pred. Link	Lich	Halted		Erratic	Forth	Lata
Appl ogic Ft		Capnograph ->	Not Hazardous	EtCO2ToApp.	EtCO2ToApp.	Not Hazardous	EtCO2ToApp. EtCO2Early	EtCO2ToApp. EtCO2I ate
	NoEtCO2			21002100200			2.00220.19	210 022010
	EtCO2Early							
	EtCO2Late							
AppLogic.	LIGOZLAIC							
				Oton 4.2				
				Step 1.3				
		Externally C	Caused Dangers			Pi	oposed Mitigatio	ons
Successor	Name	Ctrld Process	Process Var.	Intern	otation	Co-occurring	Run-time	Run-time
Danger	Name	Sidle	Name and value			Dangers	Detection	папашпу
AppLogic. EtCO2TooLow	EtCO2ToApp. EtCO2TooLow	Patient. NearHarm	Patient EtCO2 < Actual Value	sensor is lower val	than its actual	None	None	None
AppLogic.	EtCO2ToApp.			There is no fee	dback from the			
NoEtCO2	NoEtCO2	Any	Any	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.	EtCO2ToApp.	A.D.(4.004	The feedback fr	om the EtCO2	Nono	Nono	Nono
ElGOZLale	EIGOZLAIE	Ally	Ally	Sensor arrives la		none	None	None
			A - 4114	0.1	F 14 -			
			Activity	2: Internal	Faults			
				Step 2.1				
			Fa	ults Not Consider	ed			
Guid	eword				Justification			
Software Bug								
Bad Software De	esign							
Compromised S	oftware							
Compromised H	ardware	We're using a "p	roven in use" netwo	ork				
Bad Software De	esian							
Bad Hardware D	lesian							
Production Defe	ot							
Deterioration	61	Deterioration is	not a significant sou	rce of concern over	r the life of the net	working materials		
		The end ion't rec		k maintananaa		working materiale	•	
Environment dar	nages naroware	The app isit tes		K maintenance				
Operator HW Mi	stake	The network doe	esn't interact directly	with a human ope	rator			
Operator HW Er	ror		,	•				
Hacked Hardwa	re	The hospital has	s physical security m	easures in place				
Hacked Software	e		, years coounty in					
Operator SW Mi	stake	The network do	en't interact directly	with a human one	rator			
Operator SW Wr	rong Choice		Sont interact unectly	with a numan ope				
				Step 2.2				
			Inter	nally Caused Dan	gers			
Successor				Co-occurring	Design_time	Run-time	Run-time	Run-time
Danger	Guideword	Interp	pretation	Dangers	Detection	Detection	Error Handling	Fault Handling
AppLogic. EtCO2TooLow	Svntax	The EtCO2 r different syntacti the app is experimisinterprets it, reading a defla	nessage is in a c format than what ecting, so the app leading to the app ated EtCO2 value		Model Checking or Testing: Verify that syntax of			
	Syntax	. 5		None	EtCO2 values	None	Ν / Δ	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	used by Capnograph matches that used by app	попе	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	Pata Mismatch	The pulse oximeter sends EtCO2 messages faster than the app is expecting / can handle them	Nego	Static Analysis: Verify that RT / QoS	tatic Analysis: erify that RT / QoS Concurrent:		None	
AppLogic. EtCO2Late		The pulse oximeter doesn't send EtCO2 messages as frequently as the app needs them	NUTE	specifications cannot be violated	QoS Properties	If messages don't arrive as frequently as specified the app switches into a safe state and notifies the clinician	None	

			Activit	y 0: Fundam	nentals					
Elem	nent:	Successo	r Link Name:	Predecessor	Link Name(s)	Classification				
RRTO	оАрр	RRToApp	-> App Logic	PulseOx ->	RRToApp	Architectural:	Architectural: Sensor -> Controll			
			FF - 5 -							
	l	1	Activity 1	· Unsafo Int	eractione	1	1	1		
0.4			Activity I	. Onsale ill						
Step	0 1.1				Step 1.2					
	_		-		Manifestations					
Successo	r Dangers	Pred. Link	Cor	ntent Halted		Erratic		ning		
			High	Low	DDT A		Early	Late		
Appl ogic F	RTooHigh	PulseOx ->	RRTooPp.	Not Hazardous	RRToApp.	Not Hazardous	RRToApp. RRFarly	RRToApp. RRLate		
	c NoRR	Turnov opp	racionign	Not Hazardous	Norac	Not Hazardous	Triteany	Tallate		
	RREarly									
	RRI ate									
Аррсоуіс										
				Stop 1 3						
		Extornally	Sausod Dangors	Step 1.5		Dr	oposod Mitigativ	ne		
Successor		Ctrld Process	Process Var					Run_time		
Danger	Name	State	Name and Value	Interpretation		Dangers	Detection	Handling		
AppLogic.	RRToApp.	Patient.	Patient RR >	The feedback fro	m the RR sensor	-				
RRTooHigh	RRTooHigh	NearHarm	Actual Value	is higher than its actual value		None	None	None		
	RRToApp.		A	There is no feedb	There is no feedback from the RR		News	News		
AppLogic.Norr	NORR	Any	Any	ser	ISOF	None	None	None		
								Network		
								disables		
Anniaria	DDTeAre						Construct	connection (and		
AppLogic. RRFarly	RRFarly	Anv	Anv	The feedback from the RR sensor arrives earlier than it should		None	Timeouts	clinician?)		
AppLogic.	RRToApp.	,,	,,	The feedback fro	m the RR sensor					
RRLate	RRLate	Any	Any	arrives later	than it should	None	None	None		
			Activity	y 2: Internal	Faults					
				Step 2.1						
			Fa	ults Not Consider	ed					
Guide	eword				Justification					
Software Bug										
Bad Software De	sign									
Compromised Sc	oftware		We're using a "proven in use" network							
Compromised Ha	ardware	We're using a "p								
Bad Software De	sian									
Bad Hardware De	esian									
Production Defec	st.									
Deterioration		Deterioration is	not a significant sou	rce of concern ove	r the life of the net	tworking materials	5			
Environment dan	nages hardware	The app isn't res	ponsible for networ	k maintenance		0				
Operator HW Mis	stake									
Operator HW Fm	or	The network doe	esn't interact directly	with a human ope	rator					
Hacked Hardwar	~. e									
Hacked Software		The hospital has	physical security m	neasures in place						
Operator SW/ Mic	take									
		The network doe	esn't interact directly	v with a human ope	rator					
				Stop 2.2						
			I	Step 2.2	aoro					
Suggester			inter	Co consister Dan	Decign time	Dup time	Dup fires	Dun time		
Danger	Guideword	Interr	pretation	Dangers	Design-time Detection	Run-time Detection	Error Handling	Run-time Fault Handling		
20.1901	calabitord	The RR messa	ge is in a different	24.19010	2000000	2000000		. can harranny		
AppLogic		syntactic format	than what the app		Model Checking					
RRTooHigh		is expectin	g, so the app leading to the app		or Testing:					
	Syntax	reading an in	flated RR value		syntax of RR					
		-		None		None	Ν / Δ	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	попе	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	Poto Miemotok	The pulse oximeter sends RR messages faster than the app is expecting / can handle them Static Analysis: Verify that RT / QoS		Concurrent:	If messages arrive faster than allowed the network drops them and the app switches into a safe state	Nano	
AppLogic. RRLate		The pulse oximeter doesn't send RR messages as frequently as the app needs them	NUTE	specifications cannot be violated	QoS Properties	If messages don't arrive as frequently as specified the app switches into a safe state and notifies the clinician	

			Activit	y 0: Fundam	entals			
				Step 0.2				
Elen	nent:	Successor L	_ink Name(s):	Predecessor I	Link Name(s)		Classification	
				PatientToCap	onograph ->			
Capno	ograph	Capnograph	-> EtCOToApp	Capno	graph	Architectural:	Ser	isor
		Capnograph	1 -> RRToApp					
			Activity 1	: Unsafe Inte	eractions			
Ste	p 1.1				Step 1.2			
					Manifestations			
Successo	or Dangers	Pred Link	Cor	ntont	Haltod	Erratic	Tin	ning
		TTEG. LINK	001	nem	naneu	Litatic	Early	Late
EtCO2ToApp.EtCO2TooLow		PatientToCapno			DetientTeCenne		DetientTeCenne	DetiontToConno
EtCO2ToApp.NoEtCO2		graph ->	PatientToCapnog	raph.BadReading graph.NoData		Not Hazardous	graph.EarlyData	graph.LateData
EtCO2ToApp.EtCO2Early		Capnograph			5 1		5 1 1 7 1 1	5 - 1
EtCO2ToAp	p.EtCO2Late							
RRToApp.	RRTooHigh							
RRToAp	p.NoRR							
RRToApp	o.RREarly							
RRToAp	p.RRLate							
Process				Broose Values				11-1-14
	100%	000/	080/	Process values	20/	20/	10/	Dereent
Pallent ElCO2	100%	99%	90%		3%	270	170	Breaths per
Patient RR	75	74	73		2	1	0	Minute
				Step 1.3				
		Externally C	aused Dangers			Pr	oposed Mitigatio	ns
Successor		Ctrld Process	Process Var.			Co-occurring	Run-time	Run-time
Danger	Name	State	Name and Value	Interpre	etation	Dangers	Detection	Handling
EtCO2ToApp.	PatientToCapno	Dationt	EtCO2 < Actual	The sensor itsel	f malfunctions,	None		
RRToApp.	graph.	NearHarm	RR > Actual	providing an ov	ver-optimistic		None	N / A
RRTooHigh	Baukeauing		Value	reading of the p	alients nealth			
EtCO2ToApp.				The sensor stop	s providing any			
NOEtCO2	PatientToCapno	Any	None	information a	it all, so the	None	None	N/A
NoRR	graphinobata			out	out			
				The capnogra	aph's patient-		Concurrent: DT	Rollforward:
None	PatientToCapno	Any	Any	attachment produ	ices messages	None	/ QoS	Drop readings
	graph.EarlyData	,	,	faster than the ca	s them		specifications	that arrive too early
								Rollforward:
				The capnogra	aph's patient-			Notify clinician
None	PatientToCapno	Anv	Anv	attachment produ	uces messages	None	Concurrent: RT	and stop
	graph.LateData	,,	, uiy	slower than the c	apnograph itself	Hono	specifications	(transforming
				noou				this into
								1105002)
			Activity	2: Internal	Faulte			
			ACTIVIT	y z. mternal	auns			
	Step 2.1							
Faults Not Considered								
Guide Cofficiente Duce	eword				Justification			
Sonware Bug	aian							
Dau Software De	sign							
Compromised S	onware	We're using a "n	oven in use" esses	aranh				
Hardware Burg	aiuwale	were using a pr	oven in use capito	graph				
Rad Hardware D	lesian							
Bad Hardware Design								

Production Defec	ct										
Adversary Acces	ses Hardware										
Adversary Acces	ses Software	The hospital has physical security n	neasures in place								
Operator HW Mis	stake										
Operator HW Wr	ong Choice	These are no used with a superior the second second									
Operator SW Mis	stake	There are no user settings used for the caphograph									
Operator SW Mis	stake										
Syntax Mismatch	ı										
Rate Mismatch		The capnograph isn't a connection between two components									
Semantic Misma	tch										
			Step 2.2								
		Inter	nally Caused Dar	igers							
Successor	Guideword	Interpretation	Co-occurring	Design-time	Run-time	Run-time	Run-time				
EtCO2ToApp.	Guideword	A cosmic ray flips a bit in the	expression a bit in the nograph, breaking it in any possible way P		Preemptive	Compensation:	Isolation:				
RRToApp. RRTooHigh		Capnograph, breaking it in any possible way			Self-test	ECC Memory	Shielding				
EtCO2ToApp. EtCO2TooLow											
EtCO2ToApp. NoEtCO2				Compensation:							
EtCO2ToApp. EtCO2Early	Environment		Nana			Compensation:	Isolation: Adequate sealing, N/A:				
EtCO2ToApp. EtCO2Late	hardware	The capnograph is poorly	None	Testing: Subject the capnograph	Preemptive:	physiological monitors should					
RRToApp. RRTooHigh		and fails due to, eg, liquids		environmental problems	examinations	be used in case of errors with	careful use in the clinical				
RRToApp. NoRR				P		oximeter	environment				
RRToApp. RREarly											
RRToApp. RRLate											
EtCO2ToApp. NoEtCO2	Deterioration	The capnograph is poorly	None	intervals should be established	Preemptive: Routine Maintenance	None	None				
RRToApp. NoRR	Detenoration	deterioration	None	by the manufacturer							

	A	В	С	D	E	F	G	н	I	J	К
1	System:	PCA Interlock								System I	Boundary
2		Fundar	nentals							System	Environment
3		Name	Reference							PCA Pump	Patient
4										App Logic	
5	Accident Levels:	AL. DeathOrSerious Injury	N / A							Pulse Oximeter	
6										Capnograph	
7	Accidents:	Acc. PatientHarmed	AL. DeathOrSerious Injury								
8				Hazardous Factor	System Element	System Element State	Env. Element	Env. Element State			
9	Hazards:	H. TooMuchAnalg esic	Acc. PatientHarmed	Analgesic	PCA Pump	Pumping	Patient	NearHarm			
10											
11	Safety Constraints:	SC. DontODPatient	H. TooMuchAnalg esic								
12											
13					Explanations						
14	Reference				Expla	anation					
15	Acc. PatientHarmed	The patient is ha	rmed or seriously	injured as a resu	It of the App's act	ions or inaction					
16	H. TooMuchAnalg esic	The patient is given more analgesic than he / she can safely tolerate									
17	Architecture	As modeled by A	rney-etal in ICCP	S10 (in section 4	.3) with some mod	difications					
18		A lot of possibly	unmeetable assur	nptions (guarante	ed timing of netw	ork and app)					
19		Modified to inclu	de RR and EtCO2	physiological mo	onitors (in addition	n to SpO2)					

	А	В	С	D	E	F	G	н	I	
1				Activity	/ 0: Fundam	entals				
2					Sten 0.2					
3	Flem	ent:	Successor	l ink Name	Predecessor I	ink Name(s)		Classification		
4	PCA Pump		PCA Pump -> IV	Line	AppLogicComman	ds -> PCA Pump	Architectural:			
5	F		· · ·		TT - 5					
6				Activity 1	Unsafe Inte	ractions				
7	Stor	. 4 . 4		Activity		Stop 1.2				
/ Q	Step	,				Julianifostations				
0 0	Successo	r Dangers		Con	tent	annestations		Tin	ina	
10	Gubbbbbb	Bungere	Pred. Link	High	Low	Halted	Erratic	Farly	Lato	
10				riigii	LOW			Larry	Late	
			ands -> PCA	PCAPump.			PCAPump.	PCAPump.	PCAPump.	
11	SC.DontODPatie	nt	Pump	TicketTooLong	Not Hazardous	Not Hazardous	ErraticTicket	EarlyTicket	LateTicket	
12										
13	Process Variable				Process Values				Unit	
14	Ticket Duration	1	2	3	598		599	600	Seconds	
15			_	-						
16					Step 1.3					
17			Exte	ernally Caused Da	ngers			Proposed	Mitigations	
	Successor Process Var. Co-occurring						Run-time	Run-time		
18	Danger	Name	Name	Value	Interpre	etation	Dangers	Detection	Handling	
	SC.	PCAPump.			The PCA pump receives a non-zero ticket when the patient cannot tolerate any more analgesic, which leads to the pump administering drug					
19	DontODPatient	TicketTooLong	Ticket Duration	Higher than safe	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	I Due to Space Cor	straints)				
22										
23				Activity	2: Internal	Faults				
24										
25					Step 2.1					
26				Fau	Its Not Considere	d				
27	Guide	eword				Justification				
28	Compromised So	oftware								
29	Bad Hardware D	esign	We're using a "p	roven in use" PCA F	Pump					
30	Production Defec	t								
31	Semantic Mismat	ich	The PCA pump i	sn't a connection be	tween two compor	ents				
32	Adversary Acces	ses Hardware	The hospital has	physical security m	easures in place					
33				(Removed	Due to Space Cor	istraints)				
34										
35					Step 2.2					
36				Interr	nally Caused Dang	jers		1	I	
37	Successor Danger	Guideword	Interp	retation	Co-occurring Dangers	Design-time Detection	Run-time Detection	Run-time Error Handling	Run-time Fault Handling	
38	SC.		The pump is poor fails open due	rly maintained and 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 mi patient state a process, giving drug, too strong too o	sunderstands the and / or clinical either too much of a drug, or drug quickly	None	Testing: Perform user studies on the interface	None	None	Diagnosis: Thoughtful UI (re)design, periodic retraining	
40				(Removed	Due to Space Cor	ostraints)				